(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－503786
（P2000－503786A）
(43)公表日　平成12年３月28日(2000.3.28)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	３６０	
17/60			Ｌ	
		15/21	３４０Ａ	

審査請求　有　　予備審査請求　有　（全 71 頁）

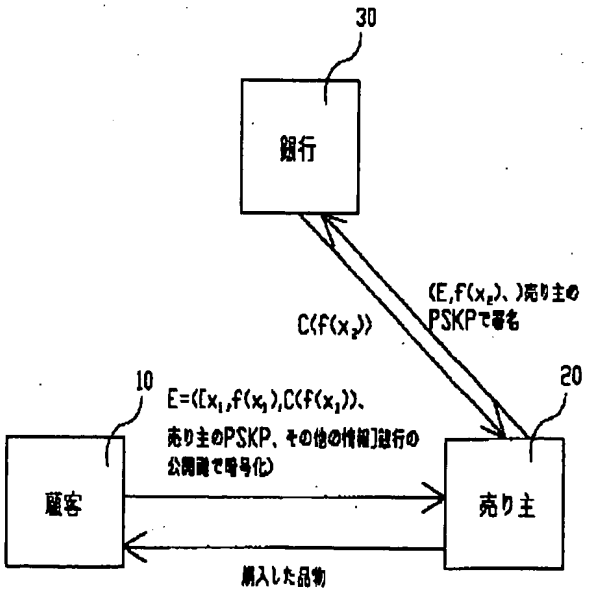
(21)出願番号　特願平9－511318
(86)(22)出願日　平成８年８月29日(1996.8.29)
(85)翻訳文提出日　平成10年３月２日(1998.3.2)
(86)国際出願番号　ＰＣＴ／ＵＳ９６／１４０７８
(87)国際公開番号　ＷＯ９７／０９６８８
(87)国際公開日　平成９年３月13日(1997.3.13)
(31)優先権主張番号　０８／５２１，１２４
(32)優先日　平成７年８月29日(1995.8.29)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＪＰ

(71)出願人　マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　98052－6399　レッドモンド　マイクロソフト　ウェイ　ワン
(72)発明者　シモン　ダニエル　アール
アメリカ合衆国　ワシントン州　98052　レッドモンド　エヌ　イー　エイティサード　ストリート　16340
(74)代理人　弁理士　関口　宗昭

(54)【発明の名称】　追跡不可能な電子通貨

(57)【要約】
電子通貨プロトコルであって、以下の手順を含む。一方向関数ｆ１（ｘ）を用いて変換前の元の値であるプレイメージｘ１から変換後の値のイメージｆ１（ｘ１）を生成する手順、イメージｆ１（ｘ１）を目隠ししない形式で第二の当事者に送信する手順、ディジタル署名を含むノートを第二の当事者から受信する手順、とからなる。前記ノートは、第二の当事者が、第二の当事者に送信したプレイメージｘ１の第一の申告者に対してあらかじめ決められた金額を信用貸しするという約束を示すものである。

図7



【特許請求の範囲】

１．電子通貨システムの実施手法であって、

一方向関数f_1（ｘ）を用いて演算前の元の値であるプレイメージx_1から演算後であるイメージf_1（x_1）を生成する手順、

イメージf_1（x_1）を見える形式で第二の当事者に送信する手順、

前記第二の当事者からディジタル署名を含む文書を受信する手順、

から成り、

前記文書が前記第二の当事者があらかじめ決められた金額を第二の当事者に対応するプレイメージｘ１の申告者に信用貸しするという確約を表すことを特徴とする電子通貨システムの実施手法。

２．第三の当事者からの商品の購入及び第三の当事者からのサービスに対する支払いとして前記プレイメージを第三の当事者へ送信する手段をさらに有することを特徴とする請求の範囲１に記載の電子通貨システムのプロトコル。

３．請求の範囲１に記載の電子通貨システムのプロトコルに加えて、

第二のプレイメージx_2を選択する手順、

第二の一方向関数f_2（ｘ）を用いて第二のプレイメージx_2からイメージf_2（x_2）を生成する手順、

第一のプレイメージx_1と目隠しされない形式のイメージf_2（x_2）を第二の当事者に送信する手順、

前記第二の当事者からディジタル署名を含む第二の文書を受信する手順、

から成り、

前記第二の文書が前記第二の当事者があらかじめ決められた金額を前記プレイメージx_2を第二の当事者に申告した者の貸し方に記入する確約を意味することを特徴とする電子通貨システムプロトコル。

４．前記第一のf_1（ｘ）と前記第二のf_2（ｘ）が同一の関数であることを特徴とする請求の範囲３に記載の電子通貨システムプロトコル。

５．第一のプレイメージx_1と目隠しされない形式の第二のイメージf_2（x_2）とを前記第二の当事者に送信する手段が匿名で行われることを特徴とする請求の範囲４に記載の電子通貨システムプロトコル。

６．前記第二の当事者が銀行であることを特徴とする請求の範囲５に記載の電子通貨システムプロトコル。

７．電子通貨システムプロトコルであってさらに、

第三の当事者からの購入品あるいはサービスに対する支払いとして第二のプレイメージｘ２が第三の当事者に送られる手順を含むことを特徴とする請求の範囲３に記載の電子通貨システムプロトコル。

８．電子通貨システムの実施方法であってさらに、

第三の当事者の署名鍵と第一のプレイメージx_1を結合してひとつの情報のブロックを作成する手順、

前記情報のブロックを第二の当事者の暗号鍵を使って暗号化しで暗号化された情報のブロックを生成する手順、

前記暗号化された情報のブロックを第三の当事者に送る手順

とからなることを特徴とする請求の範囲１に記載の電子通貨システムプロトコル。

９．電子通貨システムプロトコルであって、

第一の当事者から

第一の一方向関数f_1（ｘ）を用いて第一のイメージf_1（x_1）を生成する元の値であって、

かつ第二の当事者があらかじめ決められた金額を前記プレイメージx_1を第二の当事者に申告した当事者に信用貸しする確約と結合される第一のプレイメージを受け取る手順、

第二のプレイメージx_2を選択する手順、

第二の一方向関数f_2（ｘ）を使って第二のプレイメージx_2から第二のイメージf_2（x_2）を生成する手順、

第一のプレイメージx_1と目隠しされない形式の第二のイメージf_2（x_2）を第二の当事者に送る手順、

第二の当事者から

ディジタル署名を含む文書であって、

前記文書は第二の当事者が前記あらかじめ決められた金額を前記プレイメージｘ

２を第二の当事者に申告した第一の当事者に信用貸しする確約を意味する文書を

受け取る手順とから成ることを特徴とする電子通貨システムプロトコル。

１０．前記第一の一方向関数f_1（ｘ）と前記第二の一方向関数f_2（ｘ）が同一であることを特徴とする請求の範囲９に記載の電子通貨システムプロトコル。

１１．第一のプレイメージx_1と目隠しされない形式の第二のイメージf_2（x_2）とを前記第二の当事者に送信する手段が匿名で行われることを特徴とする請求の範囲９に記載の電子通貨システムのプロトコル。

１２．電子通貨システムのプロトコルであって、

第一の当事者から

第二の当事者の公開署名鍵と第一のプレイメージx_1を結合し一つの情報のブロックとし、前記情報のブロックを第三の当事者の暗号鍵を用いて暗号化することによって生成された暗号化された情報のブロックを受け取る手順、

第二のプレイメージx_2を選択する手順、

第二の一方向関数f_2（ｘ）を使って第二のプレイメージx_2から第二のイメージf_2（x_2）を生成する手順、

前記暗号化された情報のブロックと前記イメージｆ（x_2）を一緒にして目隠しされない形式でメッセージを形成する手順、

前記メッセージを第三の当事者へ送る手順、

第三の当事者から

ディジタル署名を含む文書であって、

前記文書は第三の当事者があらかじめ決められた金額をプレイメージｘ２を第三の当事者に申告した第一の当事者に信用貸しする確約を意味する文書を受け取る手順とから成ることを特徴とする電子通貨システムのプロトコル。

１３．前記第一のf_1（ｘ）と前記第二のf_2（ｘ）が同一の関数であることを特徴とする請求の範囲１２に記載の電子通貨システムプロトコル。

１４．前記メッセージが第三の当事者に送られる前に

第三の当事者が所有している公開署名鍵と対応する秘密の署名鍵を使って署名を行う手順により署名が行われる手順を含むことを特徴とする請求の範囲１２に記

載の電子通貨システムのプロトコル。

１５．第二の当事者が第一の当事者から暗号化された情報のブロックを受け取る

ことを特徴とする請求の範囲１２に記載の電子通貨システムのプロトコル。

１６．電子通貨システムのプロトコルであって、

第一のエンティティから

第一の一方向関数f_1（x）を用いてプレイメージx_1から生成された目隠しされない形式のイメージf_1（x_1）を受け取る手順、

あらかじめ決められた金額をプレイメージx_1の第一の申告者に信用貸しするという確約を含むメッセージを生成する手順、

前記メッセージにディジタル署名を行う手順、

第一の当事者に前記メッセージと前記ディジタル署名を送る手順とから成ることを特徴とする電子通貨システムのプロトコル。

１７．受信する当事者が第一のエンティティの口座を維持し

前記プロトコルがあらかじめ決められた金額を第一の当事者の口座の借方に記入する手順を含むことを特徴とする請求の範囲１６に記載の電子通貨システムのプロトコル。

１８．前記電子通貨システムのプロトコルがさらに続いて、

第三の当事者からプレイメージx_1を受信する手順、

前記プレイメージx_1をデータベースで調べる手順、

プレイメージx_1を前記データベースで検出しなかった場合に第三の当事者に予め決められた金額の信用貸しを行う手順、

プレイメージx_1を前記データベースに加える手順とからなることを特徴とする請求の範囲１６に記載の電子通貨システムのプロトコル。

１９．前記電子通貨システムのプロトコルがさらに続いて、

プレイメージx_1と

一方向関数f_2（x）を用いてプレイメージx_2から生成された目隠しされない形式のイメージf_2（x_2）を

第三の当事者から受信する手順と、

前記プレイメージx_1をデータベースで調べる手順と、

プレイメージx_1を前記データベースで検出しなかった場合にディジタル署名を含む署名された文書であって前記プレイメージx_2の第一の申告者に前記あらかじめ

決められた金額を信用貸しする確約を示す文書を生成する手順、

プレイメージx_1を前記データベースに加える手順とからなることを特徴とする請求の範囲１６に記載の電子通貨システムのプロトコル。

２０．前記第一の$f_1(x)$と前記第二の$f_2(x)$が同一の関数であることを特徴とする請求の範囲１９に記載の電子通貨システムプロトコル。

２１．第二の当事者から

第三の当事者の暗号鍵と第一のプレイメージx_1とをひとつの情報のブロックに結合して生成され、第一の暗号鍵を用いて前記情報のブロックを暗号化して暗号化された第一のブロックを形成し、一方向関数$f_2(x)$を用いてプレイメージx_2から生成された目隠しされない形式のイメージ$f_2(x_2)$と前記暗号化された第一の情報のブロックを結合したメッセージを受信する手順、

前記暗号化された第一の情報のブロックを解読する手順、

ディジタル署名を含む文書であって、前記プレイメージx_2の第一の申告者に予め決められた金額の信用貸しを行うという確約を表した文書を作成する手順、

前記文書を第二の当事者に送る手順とからなることを特徴とする請求の範囲１６に記載の電子通貨システムのプロトコル。

２２．前記第一の$f_1(x)$と前記第二の$f_2(x)$が同一の関数であることを特徴とする請求の範囲２１に記載の電子通貨システムプロトコル。

２３．前記電子通貨システムのプロトコルがさらに、

プレイメージx_1をデータベースで調べる手順、

プレイメージx_1を前記データベースで検出しなかった場合にのみ署名された文書を作成する手順、

プレイメージx_1を前記データベースに加える手順とからなることを特徴とする請求の範囲２１に記載の電子通貨システムのプロトコル。

２４．電子通貨システムのプロトコルであって、

第一のイメージｆ（x_1）と

予め決められた貨幣価値と関連づけられた第一のプレイメージx_1とを入手する手順、

第二のプレイメージx_2を選択する手順、

第二の一方向関数f_2（ｘ）を用いて第二のプレイメージx_2から第二のイメージf_2（x_2）を生成する手順、

第一のプレイメージx_1と目隠しされない形式の第二のイメージf_2（x_2）を第二の当事者に送る手順、

第二の当事者から

ディジタル署名を含む文書であって

第二の当事者が予め決められた金額であって前記予め決められた貨幣価値を超えない金額を

第二の当事者に前記第二のプレイメージx_2を最初に申告した者に信用貸しするという確約を表した文書を受け取る手順からなることを特徴とする電子通貨システムのプロトコル。

２５．前記予め決められた金額が前記予め決められた貨幣価値よりも少ないことを特徴とする請求の範囲２４に記載の電子通貨システムのプロトコル。

２６．前記第一の一方向関数f_1（ｘ）と前記第二の一方向関数f_2（ｘ）が同一であることを特徴とする請求の範囲２４に記載の電子通貨システムのプロトコル。

２７．電子通貨システムのプロトコルであって、

第一のイメージｆ（x_1）と

予め決められた貨幣価値と関連づけられた第一のプレイメージx_1とを入手する手順、

正の整数１からｎの値を持つ多数のプレイメージx_iを選択する手順、

第二の一方向関数f_2（ｘ）を用いて第二のプレイメージx_iから多数のイメージf_2（x_i）を生成する手順、

第一のプレイメージx_1と目隠ししない形式ですべてのイメージ$f_2(x_1)$を第二の当事者に送る手順、

第二の当事者から

各文書がディジタル署名を含み前記文書の数はイメージ$f_2(x_1)$と同じである多数の文書であって予め決められた額が多数記載されており、

前記多数の文書のそれぞれには第二の当事者がプレイメージx_1の第一の申告者に対して

異なった額の前記予め決められた額が多数記載されているもののうち前記プレイメージx_1と対応する額を信用貸しするという確約を表した文書を受け取る手順とから成り、

前記予め決められた額の総計が前記予め決められた貨幣価値と等しいことを特徴とする電子通貨システムのプロトコル。

２８．電子通貨システムのプロトコルであって、

第一のイメージ$f(x_1)$と

予め決められた貨幣価値と関連づけられた第一のプレイメージx_1とを入手する手順、

第一のプレイメージx_1と第二の当事者の署名鍵を結合して一つの情報ブロックを作成する手順、

前記情報ブロックを第三の当事者の暗号鍵を用いて暗号化された情報のブロックとして生成する手順、

第三の当事者に暗号化された情報のブロックを送る手順とから成ることを特徴とする電子通貨システムの実施方法。

２９．前記電子通貨システムのプロトコルがさらに、

第二の当事者のその他の情報と署名鍵と第一のプレイメージx_1をひとつの情報のブロックに結合する手順を含むことを特徴とする請求の範囲２８に記載の電子通貨システムのプロトコル。

３０．電子通貨システムのプロトコルであって、

一方向関数$f_2(x_2)$を用いてプレイメージx_2から生成された

目隠しされない形式のイメージf_2（x_2）を

第二の当事者に送る手順と、

第二の当事者から

ディジタル署名を含む目隠しされない形式の文書であって

前記プレイメージx_1を最初に申告した者に対し予め決められた金額の信用貸し

を行うという確約を表した文書を受け取る手順、

第二の当事者から前記目隠しされない形式のノートを受け取った応答として品物

やサービスを第三の当事者に提供することを許可する手順とから成ることを

特徴とする電子通貨システムのプロトコル。

【発明の詳細な説明】

追跡不可能な電子通貨

背景技術

この発明は、電子通貨システム一般に関する。

電子通貨システムの直観的にわかる最終的な形態は、有形の現金の最良の特徴（プライバシーが守られる、匿名性、偽造しにくい）と、電子取り引きの持つ最良の特徴（速さ、簡便性、輸送や保管に対する潜在的な安全性）を合わせ持った形態である。匿名性を有す電子通貨システムを実現するための基本的な問題は、次のように単純化することができる。２つの連続した取り引きにおいて、この電子通貨の所有者が識別できなかったならば、この所有者が第一の取り引きがなかったように振る舞い、同じ電子コインを再び使用することをどうやって防ぐかという問題である。この問題に対する第一の解決方法は、チャーム、フィアットとノアーによって提案されている（D．チャーム(D.Chaum)、A．フィアット(A.Fiat)、M．ノアー(M.Noar)著、アントレーサブル・エレクトロニック・キャッシュ(Untracedable Electronic Cash)、Proc. CRYPTO'88、Springer-Verlag(1990)、319-327ページ）。これは、同じ電子通貨が２回、中央の銀行に送られてきた場合には、通貨の二重使用を検出して二重使用を行った人の特定が十分に行えるということを前提条件として成立している。他のいくつかにもこの前提が用いられていて、銀行は各取り引きを複雑にする必要がないという利点を有す。しかしながら実際には、この前提条件には重大な欠点がある。それは不正な取り引きは発生後しばらくたってから検出されるということであり、不正実行者が法によって処罰されないという確信があれば（アクセスできない状態であったり、第三者のＩＤや電子通貨を使っている場合など）、不正実行者は意のままに電子通貨の二重使用をすることができる。

しかしながら、このような電子通貨の不正使用を防止するには、二重使用の検出や、二重使用に対して警告を発することができるように、取り引きが発生する毎に何らかの確認をいずれかの方法で行う必要がある。それでは、どのようにして匿名性を保護するのか。ひとつのアプローチとして、中身にいたずらできない

ように作られたハードウエアを基礎として、電子通貨を使う人が正直に（すなわち、電子通貨の二重使用をしない）しなければならないよう強いる方法がある(例えば、S.イーブン(S.Even)、O.ゴールドリッチ(O.Goldreich)、Y.ヤコブ(Y.Yacobi)著、エレクトロニックウォーレット(Electronic Wallet,Proc. CRYPTO'83、Plenum Press(1984)、383-386ページを参照のこと)。しかしながらこのような前提に基づいた方法は、非常にもろい。もし誰かがハードウエアの不正操作に成功したらならば、その不正使用者が通貨の二重使用ができるばかりでなく、ハードウエアに隠された情報を手に入れる（たとえば、購入したり、偶然によって）ことができれば、誰でもがどこからでも勝手に高額な金額を使うことができるようになる。従来の不正使用防止技術は、前述のようなリスクを有すものを基礎としたものであるため、信頼できる技術ではない。

その他のアプローチとして、暗号による方法がある。例えば、ある強力な暗号法のもとでは、「目隠しされた」通貨と、後で正規通貨であると認証できるが、どのように特殊なプロトコルを実行させても接続できない情報を造るプロトコルを構築することが可能となる。（例として、D.チャーム(D.Chaum)著、プライバシー・プロテクト・ペイメント(Privacy Protected Payments--Unconditional Payer and/or Payee Untraceability,SMART CARD 2000: The Future of IC CardsOOProc.ifip wg 11.6 Int'l Conf.,North-Holland(1989), ページ69-93)、及びD.チャーム(D.Caum)著、オンライン・キャシュ・チェック(Online Cash Checks)、Proc.EUROCRYPT'89、Springer-Verlag(1989)、288-293ページを参照のこと）

発明の開示

この発明は、簡単で実用的なオンライン電子通貨システムであって、匿名性を有し追跡不可能な情報伝達が可能なネットワークを基礎とした電子通貨システムを実現するものである。概して、この発明には２つの簡単な基本要素である、一方向関数と署名機構を用いている。どちらもよく知られた技術であって、詳細については、一般に入手できる暗号に関する本で知ることができる。例えば、ブルース・シュネイヤー（Bruce Schneier）著、アプライド・クリプトグラフィー（

Applied Cryptography)（１９９４年　ジョン・ウィリー・アンド・サンズ 社 (John Wiley & Sons, Inc.) 刊にある。このシステムは、電子通貨を使う人の匿名性を保護することはもちろん電子通貨の正当性を保証するものであり、偽造することはできず、また１回しか使用できない。

本発明の一形態である電子通貨プロトコルは、一方向関数 f_1（x）を用いて変換前の元の値であるプレイメージ x_1 から変換後の値であるイメージ f_1（x_1）を生成する手順、イメージ f_1（x_1）を目隠ししない形式で第二の当事者に送信する手順、第二の当事者からディジタル署名を含む文書を受け取る手順とから成る。前記受け取った署名を含む文書は、第二の当事者が、第一のプレイメージ x 1 を決めた者に対してあらかじめ決められた金額を信用貸しするという確約を意味する。

本発明の最良の形態は、次に示すような形態を含む。本発明の電子通貨プロトコルはまた、第三の当事者から購入した商品や受けたサービスに対する支払いとして、プレイメージ x_1 を第三の当事者へ送る場合も含んでいる。またさらに、第二のプレイメージ x_2 を選択し、第二の一方向関数 f_2（x）により第二のプレイメージ x_2 を第二のイメージ f_2（x_2）に変換し、第一のプレイメージ x_1 と目隠ししない形式で第二のイメージ f_2（x_2）を第二の当事者に送信し、第二の当事者からディジタル署名を含む文書を受信するという形態もある。前記文書は、第二の当事者が、第一のプレイメージ x_2 を決めた者に対してあらかじめ決められた金額を信用貸しするという確約を意味する。どちらの場合も、f_1（x）と f_2（x）は同じ関数である。後者の場合、第二の当事者に対して第一のプレイメージ x_1 と目隠ししない形式で第二のイメージ f_2（x_2）を送信しているのは、匿名性を保持するためであり、第二の当事者は銀行である。

また、本発明の最良の形態であるプロトコルには、第三の当事者の署名鍵と第一のプレイメージ x_1 を結合して情報をひとつのブロックに構成する手順、前記情報ブロックを第二の当事者の暗号鍵を使って暗号化して、暗号化された情報ブロックとする手順、前記暗号化された情報ブロックを第三の当事者に送信する手順とから成るものがある。

その他の形態である本発明の電子通貨プロトコルは次の手順で行われる。まず第一の当事者から第一のプレイメージx_1を受け取る手順であり、このプレイメージx_1は第一の一方向関数$f_1(x)$によって処理され第一のイメージ$f_1(x_1)$となる。前記第一のプレイメージx_1は、第二の当事者が前記第一のプレイメージx_1を第二の当事者に申告した第一の当事者に対して、予定額の信用貸しを行うという、第二の当事者による確約と連結している。さらに、第二のプレイメージx_2を選択する手順、第二の一方向関数$f_2(x)$により第二のプレイメージx_2から第二のイメージ$f_2(x_2)$を生成する手順、第一のプレイメージx_1と目隠しされない形式の第二のイメージ$f_2(x_2)$を第二の当事者に送信する手順、第二の当事者からディジタル署名を含むノートを受信する手順とから成る。このノートは、第二のプレイメージx_2を第二の当事者に送った第一の当事者に対し、予定の額の信用貸しを行うという第二の当事者の約束を表わしている。

さらなる他の形態では、本発明の電子通貨プロトコルは次の手順で行われる。まず、第一の当事者から暗号化された情報のブロックを受け取る手順であり、この情報が暗号化されたブロックは、第二の当事者の公開署名鍵と第一のプレイメージx_1とを連結して情報のブロックが構成され、さらに前記情報のブロックは第三者の暗号鍵を使って暗号化されたものである。続いて、第二のプレイメージx_2を選択する手順、第二の一方向関数$f_2(x)$を用いてプレイメージx_2からイメージ$f_2(x_2)$を生成する手順、前記暗号化した情報ブロックとイメージ$f_2(x_2)$を含むメッセージを目隠ししない形式で作り上げる手順、前記メッセージを第三の当事者に送る手順、第三の当事者からディジタル署名を含むノートを受け取る手順から成る。このノートは、第二のプレイメージx_2を第三の当事者に送った第一の当事者に対し、予め決められた額の信用貸しを行うという第三の当事者の確約を表わしている。

さらなる他の形態では、本発明の電子通貨プロトコルは次の手順で行われる。第一のエンティティから一方向関数$f_1(x)$をプレイメージx_1に適用して生成され、かつ目隠しされない表記形式のイメージ$f_1(x_1)$を受信する手順、プレイメージx_1を送った第一の当事者に対し、予め決められた額の信用貸しを行うという確約を含むメッセージを作成する手順、前記メッセージにディジタル署名

で

署名する手順、前記メッセージをディジタル署名と一緒に前記第一の当事者に送信する手順、とである。

本発明の電子通貨プロトコルの最良の実施の形態ではさらに続いて、第三の当事者からプレイメージx_1を受け取る手順、プレイメージx_1をデータベースで調べる手順、もしプレイメージx_1がデータベースになかったら、あらかじめ決められた金額を第三の当事者に信用貸し、プレイメージx_1をデータベースに加える手順が含まれている。あるいは本発明の電子通貨プロトコルがさらに続いて、プレイメージx_1と目隠しされない形式のイメージ$f_2(x_2)$であって一方向関数$f_2(x)$をプレイメージx_2に適用して生成されたイメージを第三者から受け取る手順、プレイメージx_1をデータベースで調べる手順、もしプレイメージx_1がデータベースになかったら、あらかじめ決められた金額をプレイメージx_2を送った第一の当事者に信用貸しするという確約を示し、ディジタル署名も添付されているノートを作成する手順、プレイメージx_1をデータベースに加える手順から成るプロトコルであってもよい。

また本発明の最良の実施の形態として、次に示すメッセージを第二の当事者から受け取ることを特徴とするものがある。前記メッセージは、第三の当事者の暗号鍵と第一のプレイメージx_1とを結合してひとつの情報のブロックとして形成し、前記情報のブロックを第一の暗号鍵を使って暗号化された第一のブロックを生成し、前記暗号化された第一のブロックをプレイメージx_2を一方向関数$f_2(x)$を用いて生成される目隠ししない形式のイメージ$f_2(x_2)$と結合することによって得られる。さらに、暗号化された第一の情報のブロックを解読する手順、ディジタル署名を含み、第一のプレイメージx_2の申告者にあらかじめ決められた金額を信用貸しするという確約を表わしたノートを生成する手順、前記ノートを第二の当事者に送る手順を有している。

また、さらに他の形態として、次の手順を有する電子通貨プロトコルがある。一方向関数$f_2(x)$を用いてプレイメージx_2から生成され目隠しされない形式のイメージ$f_2(x_2)$を第二の当事者に送る手順、第二の当事者から署名された

ノートであって、目隠しされない形式で、ディジタル署名を含み、最初にプレイメージx_2を申告した者に対して決められた金額の信用貸しを行う約束を表わした

ノートを受け取る手順、さらに前記目隠しされない形式のノートを第二の当事者から応答として受け取り、品物やサービスを第三の当事者へ配達するのを認める手順とがある。

本発明は、簡単で安価な、擬似貨幣による取り引きの方法を提供するものである。交換（例えば貨幣の引き出し）といった項目では、実際の貨幣と同じ特性を持つ。例として、本発明は、（１）大体において匿名性が保証されている、（２）安全で、（３）安価で使うことができ、（４）持ち運びが簡単で交換も容易である、という特徴がある。

関係者は、ある特定の貨幣に対するx_1の値を貨幣を使うまで秘密にしておくことにより、その貨幣支払いの取り消しといった不正な銀行の背信行為から守られている。特定の金額ｆ（x_1）が公にかつ匿名でなく預金されている限り、x_1と結合している支払いが行われるまで、銀行には道義心が要求される。もちろん、銀行は、受け取ったx_1がすでに使われた貨幣に関したものであると主張して、実際の交換処理中に匿名での交換処理を取り消しを行うことができる。しかしながら、銀行は誰がこのような「食い逃げ」計画によってだまそうとしたか知ることができない。それ故、銀行はモニターや一般に公表されることに対して無防備である。

最終的に、電子通貨の署名に用いられるディジタル署名手法の有す安全性により、銀行も電子通貨の偽造から守られる。さらに加えて、銀行は、貨幣に対するx_1の値を永久に保存していることにより、「二重使用（あるいは二重支払い）」を防止する。

その他の利点や特徴は、以下の発明の実施するための最良の形態及び請求の範囲において明らかにする。

図面の簡単な説明

第１図は、匿名でない電子通貨の引き出しプロトコルを示す図である。第２図

は、電子通貨の匿名での交換プロトコルを示す図である。第３図は、電子通貨での匿名での商品購入プロトコルを示す図である。第４図は、匿名でない電子通貨の預金プロトコルを示す図である。第５図は、電子通貨の匿名での支払いプロトコルの他の形態を示す図である。第６図は、匿名あるいは匿名でないドロップ・ペイメントまたは為替プロトコルを示す図である。第７図は、暗号化した為替プロトコルを示す図である。

発明を実施するための最良の形態

匿名で通信する能力は、いろいろな意味で、匿名の金銭取り引きが行われる場合には優先されなければならない事項である。なぜなら、ある団体の通信についての情報は、その団体の商取り引きに関する情報を明らかにしてしまうからである。実際には、通信の匿名性が基礎としているのは、電話会社が自社のシステムの秘密性を保護しているという信頼にすぎない。各団体は正体のわからない匿名での返信者を信頼するか、あるいは文献から公に入手できる他の技術のひとつを装備して信頼するかの選択ができる。

団体間の通信は第三者に対して匿名性を持つばかりでなく、その団体間でも互いに匿名性を持って通信を行うことを想定する。（代表的な実施例において、後者の形態は自己認識を除いて前者の自然な結果である。）このような条件における、簡単で幾分匿名性を有す電子通貨システムのプロトコルを第１図に示す。

以下で説明するさまざまなプロトコル（第１図から第７図を参照のこと）では、３団体を顧客１０と売り主２０と銀行３０という名称で定義する。顧客１０は、もちろん一般的には支払人の代表であり、売り主２０は一般的には受取人の代表である。当然ではあるが、この設定は説明を明快にする目的で決めたもので、この発明の範囲を限定するものではない。従って当然ながら、この三者を集団Ａ、集団Ｂ、集団Ｃとして引用しても同じ効力を持つ。

図には、いくつかの異なった団体がブロックによって示されており、ある団体から他の団体への情報の伝達は該当するブロックをつなぐ線によって示している。各線は、ある団体から他の集団へ一定の情報が伝わることを示しており、線の端の矢印が通信の方向を示している。伝達される情報は、内容をまとめたシンボ

ルとして、線の下に示してある。

各ブロックにはラベルが付けられ、次に示すような特定の物として記述されているが、前記特定の物による処理は、コンピュータ処理や通信を実行するコンピュータ機器によって実行されるものである。コンピュータ機器は、多岐にわたる種類の電子機器を含んでいる。例えば、パーソナル・コンピュータ、ＰＣカード（ＰＣＭＣＩＡ対応カード）、ＰＤＩ、スマートカード、パームトップコンピュータ、強力なワークステイション等でありこれらはその一部に過ぎない。次に説明するように、プロトコルの銀行側の処理は、現在ＡＴＭによるトランザクションを処理しているサーバと同様に、電子商取引を処理するようにプログラムされたサーバによって実行される。前記サーバは、データの到着する複数の電話線を有し、関連データを保存するためのデータ記憶容量を持っていることが望ましい。

コンピュータ機器が内部あるいは外部に、プロトコルを実行するするために必要なプログラムやデータのために必要なメモリを有していることは当然のことである。さらに、前記コンピュータ機器は、例えばモデムのような、他のコンピュータ機器と通信を行うための手段も有す。さらに付け加えれば、情報を伝送する通信媒体は非常に多くの可能性を持っている。媒体の例としては、電話線、ケーブル、インターネット、衛星通信、無線通信などが挙げられる。言い換えれば、本発明は、使われている機器の種類や採用している通信方法によって限定されるものではない。可能性や組み合わせは、人の創作力によって限定されるものである。

これから説明するプロトコルにおいては、銀行３０が公に使用できる一方向関数ｆ（ｘ）を、選択し、制定する。このような関数は、誰もが商取引においてアクセスし使うことができるように、誰でもが公に入手できるものでなくてはならない。一般に、一方向関数は、x_1を使ってｆ（x_1）を算出することはできるが、ｆ（x_1）を与えられてもx_1を算出できない関数ｆ（ｘ）を意味する。以下の説明では、x_1はｆ（x_1）のプレイメージと、ｆ（x_1）はx_1のイメージとする。

実際には、完全な一方向関数は存在しない。現在一方向関数と考えられているすべての関数は、コンピュータの能力や手法によってｆ（x_1）からx_1を決定することが十分にできる。それゆえ、一方向関数という語には、ｆ（x_1）からx_1を算出することが、不可能である必要はないが非常に難しい関数であるという意味も含まれる。

一方向関数は、標準のハッシュ関数（例えば、ＭＤ５、ＳＨＡ等）のうちのいずれかでよい。さらにつけ加えれば、いくつかの一方向関数を使うことも、これを結合することも可能である。この技術分野において、多くの一方向関数が知られている。その中の幾つかは、コンピュータに移植することが簡単で、スマートカードに装備することもできる。

以上の基礎知識を前提として、本発明の実施の形態となる種々のプロトコルについて説明する。まず、顧客が銀行から「キャッシュ」を手に入れる処理に用いられる電子通貨の引き出しプロトコルから始める。

引き出しプロトコル

電子通貨の引き出し処理は、第１図に示した手法に従って行われる。顧客１０は、任意の数x_1を選び、一方向関数ｆ（ｘ）を使って変換後の値であるx_1のイメージを生成する。x_1の値は後処理装置が任意で行っているような乱数発生手段から得られた無作為の数列である。この数列は、例えば１２８ビット長のデータである。顧客１０は、支払い処理が発生してから完了するまでこれを秘密にしておく。

顧客１０は、金額とｆ（x_1）をまとめて銀行３０に送って引き出しの要求を行い、銀行３０から金を引き出す（匿名ではなく）。銀行３０は、明細書にディジタル署名を行って顧客の趣意に従う。このようにｆ（x_1）を正規の電子通貨として認定し、要求の額を、顧客１０が銀行３０に持っている口座の借方に記入する。言い換えれば、銀行３０は、「最初にｆ（x_1）のプレイメージを決めた者に対して、総額ｚの信用貸しを行う」ことに関して銀行３０は署名を行って証明する、という効力を表わす明細書あるいは覚え書きを発行する。

署名や情報の認証を行う技術（例えば、秘密鍵と公開鍵のペアを使う方法）や

、ディジタル署名の手法は、よく知られている技術である。さらに詳しくは、この分野において広く認められた参考文献を参照すればよい。例えば、ブルース・シュネイヤー(Bruce Schneier)著、アプライド・クリプトグラフィー(Applied Cryptography)、１９９４年　ジョンウイリー・アンド・サンズ社(JohnWiley&Sons,Inc.)などである。

一般的に署名機構とは、文字にタグを付けるやり方のことである。典型的な例としては、公開鍵と秘密鍵のペアを使うものがある。公開鍵及び秘密鍵は、一方向関数を使って実行される。より現実的なアプローチ方法としては、さらに効果を上げるためにトラップ・ドア機能を使う方法がある（例えば、スキネイナー(Schneiner)著、ＲＳＡ、ＤＳＳ、エルガマ・アルゴリズム(RSA, DSS, Elgamal algorithms)参照のこと）。秘密鍵は、文字か文字列を暗号化するのに使われ、文字に添付するディジタル署名として使われる。ディジタル署名は、自身の秘密鍵を持っている者の署名であることを示している。なぜなら、他者が前記文字列からこのような署名を作り出すことはできないからである。第二の当事者が公開鍵を使ってタグの暗号を解読すれば、署名者自身の秘密鍵によって署名がなされたことがわかる。この手法を保証するために、署名をした人の公開鍵を誰もが手に入れまた預けられてこと、かつ秘密鍵は危険にさらされることはないと信頼できることが、前提となっていることは明らかである。

公開鍵を公表すること、及び銀行３０が第一のｆ（x_1）のプレイメージを決めた者に対して明記された額を支払うという覚え書きにディジタル署名を添付したことにより、銀行３０はその責任を明らかにし、さらに偽造者から自身を守る。

銀行が発行した、証明書となる覚え書きをここではＣ（ｆ（x_1））と定義し、ノートと呼ぶ。このノートは顧客１０に返送される。さらに付け加えれば、それは公然と入手することができるが、x_1を知らない人にとっては何の価値もない。

交換プロトコル

関係者（例えば、顧客１０や売り主２０）は、いつでも、銀行３０において匿

名で電子通貨の「交換」ができる。実際には、相手側当事者から電子通貨を受け取ったら、処理を迅速に行うことが特に重要である。これは、電子通貨の正当な受取人の前に誰か他の者がx_1を銀行３０に送信してしまうリスクを最小にするためである。不正実行者は、複数の者に対してx_1を送信し、その電子通貨を複数回、送信しようとするかもしれない。そのようなことが起きたら、銀行３０に届いた最初の受取人がその価値を受け取り、その他の電子通貨の受取人達は該当しない電子通貨となり交換することができない。売り主２０にとっては、交換のタイミングはさほど重要でない。なぜなら、大体において売り主２０は、電子通貨の受

け取りが有効に完了するまでは、納入予定の品物やサービスを提供しないからである。　第２図に示したように、顧客１０が電子通貨を匿名で交換することを望んだと仮定すると、顧客１０は銀行３０にx_1と任意に選ばれたx_2の変換後のイメージである$f(x_2)$を送信する。言い換えれば、顧客１０はx_1によって前述したような引き出しプロトコルを行い、同時に引き出した総額を提供する。銀行３０は単に$f(x_2)$を認証し、$f(x_1)$は「すでに使われた」ということの証明としてx_1をデータベース４０に保存するだけである。これがx_1の二重使用されるのを防止する交換の手法である。

$f(x_1)$と$C(f(x_1))$はすでに銀行３０が所有しているので、銀行３０に対してx_1と$f(x_2)$といっしょにその情報を送ることは任意である。

プロトコルの銀行側処理がサーバーに実装されていれば、これは受信したx_1を自動的に保存する。さらに、銀行３０がもうひとつのx_1を受け取る毎に、最初にそれがすでに使われたもの（すなわち受信されたもの）であるかをチェックする。

誰が実際に電子通貨を使っているのかがはっきりわからない交換処理を、連続して取り扱うことができるようになる。交換処理には$f(x_2)$を明らかにすることのみが必要であり、x_2の持ち主を明らかにする必要はないことに注目してほしい。匿名を実現するための他の手法と違って、電子通貨を目隠しすること等その他の処理を必要としない。実際には、$f(x_1)$が目隠しされず、広く一般

に知られていることが望ましい。

通信の匿名性を確保するよう求める手法は何でも、処理の匿名性が確保されれば十分に目的を果たす（すなわち、匿名性を実現することは可能であるが必須ではない）。

この手法は、電子通貨を両替する方法として使うこともできる。ｆ（x_2）を送信する代わりに、両替をしようとしている者は、複数のｆ（ｘ）の値（例えは、ｆ（x_2）、ｆ（x_3）、ｆ（x_4））を送信することができる。これらは、個々に特定の値を持ち、総合するとｆ（x_1）の値と関連する。銀行は、複数の署名付きノートであるＣ（ｆ（x_1））を返送する。

購入プロトコル

第３図に示したように、実際に電子通貨を支払うプロトコルは交換プロトコルと似ている。支払いを行う者（例えば顧客１０）は、受け取り人（例えば売り主２０）に、x_1を渡す。売り主２０は直接あるいはすぐにｆ（x_1）あるいはＣ（ｆ（x_1））にアクセスすることができないので、顧客１０は取引の一部の情報として送る。売り主２０は銀行３０に直接要求して、x_1を「フレッシュな」金銭に換える。この時当然に、銀行３０はx_1が以前に使われたものでないことを最初に確認する。売り主２０がこの交換処理を実施するときには、第２図に示した交換プロトコルを使う。前記交換処理が引き受けられた後、売り主２０は購入された品物あるいはサービスを顧客１０に提供する。

預金プロトコル

第４図に示したように、使用しない貨幣はいつでも、銀行３０に匿名でなく預金することができる。例えば、売り主２０が使わない貨幣ｆ（x_1）を預金しようとした場合、x_1を預金の要求と共に銀行３０に送信する。売り主２０は、ｆ（x_1）はもちろんＣ（ｆ（X_1））を任意で送ってもよい。

x_1と預金要求を受け取ると、銀行３０はx_1が以前に銀行に送られてきたことがあるかどうか、データベースを調べる。もちろん、以前に送られてきたことがあれば、銀行３０は売り主の請求書を信用せず、売り主２０に対して正規の電子通貨ではないことを報告する。銀行３０が以前にx_1を受信したことがなければ

、あらかじめ決められ金額がある請求書を信用し、信用取引が登録されたことを確認するために預金の受領書を売り主２０に送る。

プロトコルの拡張

以上説明した電子通貨手法における交換及び支払プロトコルには、いくつかの他の実施の形態の例がある。これら他の実施の形態は、求められている匿名性のレベルや関係に応じた有効な手段となるように作られている。例えば、第５図に示したのは、顧客１０が売り主２０よりも銀行３０にアクセスするほうが容易である場合、売り主２０は最初に顧客１０にｆ（x_2）を送り、顧客１０は売り主２０の代わりに交換プロトコルを行い、支払いの証明として署名された電子通貨

、

例えばＣ（ｆ（x_2））を返送する。前述したように、交換プロトコルは匿名で行われる。

あるいは、顧客１０及び売り主２０の双方が、お互いよりも銀行とよい関係をもっている場合、図６に示したような「ドロップ」ペイメントプロトコルを使うとよい。このプロトコルに従えば、顧客１０は売り主２０のための支払いを銀行に降ろし、売り主２０はその後すぐに銀行から支払いを回収する。

「ドロップ」支払いプロトコルの手順を以下に示す。最初に、顧客１０がある特定の額の貨幣の代わりとしてのx_1を銀行３０に送る。この時、売り主２０の公開署名鍵ｐ（ＰＳＫＰ）と取り引きに関する情報を付加して送る。いろいろな情報があるが、例えば、顧客１０が購入した品物を明らかにしたり取り引きを確認することを望んだ場合、さらに/あるいは売り主が支払いに関する顧客の意向を認めたといことを指示する場合などがあり、その結果、電子通貨が本質的な意味において、「電子為替」に変る。顧客１０は任意でｆ（x_1）とノートＣ（ｆ（x_1））を送ってもよいが、前述したように、この情報はすでに銀行３０が入手しているので、送る必要はない。

顧客１０が提供したその他の情報から集められた記録は、遠隔支払設定として特定の用途に使えるかもしれない。取り引きの性格が特に暗黙であるという場合でなければ、典型的には個人的な支払い方法になる。

もし、売り主２０が匿名性を保持することを望まなければ、公開署名鍵は売り主２０のＩＤと明らかに関係しているものであってよいが、もし匿名性を望むのであれば、公開署名鍵はＩＤとはまったく関係ない特別な目的を有した公開鍵としなければならない。後者の場合には、公開鍵は信頼できる知人に極秘に渡すか、単純に匿名で公表する。

銀行３０はｘ１に付随した第一の電子通貨ｆ（x_1）として表わされた総額を渡すことに同意し、以前に配布された公開署名鍵ｐと対応する秘密の署名鍵を使って署名されている。このようにして、顧客１０が購入しようとした品物の支払いを手に入れるために、売り主２０は、第１図に関連して以前に記述したプロトコルを使って、銀行３０から金を引き出す。このとき、売り主２０は任意のx_2を選択し、ｆ（ｘ）を使ってイメージｆ（x_2）を生成する。しかしながらこの例では、

売り主２０はｆ（x_2）を銀行３０に送信する前に秘密署名鍵を使ってｆ（x_2）に署名を行う。付け加えると、この場合、貨幣は売り主の口座から引き出されるのでなく、顧客１０によってこの処理の前に与えられた口座から転送するだけである。

銀行３０は売り主の公開署名鍵を使って、受信したｆ（x_2）が売り主２０（すなわち貨幣の転送を行った者）によって署名されことを確かめる。ｆ（x_2）の署名を確認すると、銀行３０は売り主２０に送信するノートＣｆ（x_2））を発行する。

金を受け取ったという確認のノートＣ（ｆ（x_2））を売り主２０が受け取った後、売り主２０は顧客１０に品物を送る。

もちろん理論上は、銀行３０は支払先に金を与える代わりに金を自分のものにすることによってだますことができる。しかしながら、支払人の匿名性を信頼している、あるいは少なくとも一般の人々が銀行３０が不正しないことをモニターしているので、支払人が取り引きを暴露する可能性をあてにすることができる。

関係者間の通信が傍受されているという設定のもとで、交換プロトコルを安全なものにする、とりわけ秘密のｘの値をが立ち聞きする者を通り抜けて通過する

いくつかの方法がある。最も自然な方法は、公開鍵による暗号法である。関係者が銀行のものはもちろんのこと互いの公開暗号鍵を知っていれば、銀行３０が送信するものを除くすべてのメッセージが、受信側の公開暗号鍵を使って暗号化するか、受信側の公開暗号鍵を使って暗号化された相称的な「セッションキー」を使っているかぎり、前述した全てのプロトコルが立ち聞きするものを絶滅させるように機能する。もちろん銀行のメッセージは、秘密でなくてよいよう考慮されている。なぜならメッセージは、x_1が誰か他の者によって秘密にされているｆ（x_1）という形式の署名された貨幣だけで構成されているからである。暗号化処理時にメッセージの認証コードやＭＡＣを使えば、メッセージが目的地に到着するまで送り主以外の誰かによっていたずらされることはないことが保証される。

公開暗号鍵の使用により、別の種類の「電子為替」が可能となる。この事例を第７図に示し、暗号化された電子為替プロトコルとして一般にあてはめる。顧客１０は、ある正規の電子通貨としての秘密のx_1の値を、売り主２０の公開鍵ｐと

その他の必要なＩＤや取引情報といっしょに暗号化する。前述の「ドロップ」プロトコルの場合と同様である。顧客１０はこの情報を、銀行の公開暗号鍵を使うか、あるいは銀行の公開暗号鍵を使って暗号化されたセッションキーを使って暗号化する。その後、顧客１０は暗号化された情報を直接売り主２０に送信する。

これを「現金」にするために、売り主２０は任意の値x_2を選び、そのイメージｆ（x_2）を生成し、顧客１０から受信したメッセージＥにｆ（x_2）を添付する。前と同様、ｆ（x_2）は銀行によって署名されると、それは売り主２０への金の移転を意味する。売り主２０は完了メッセージ（あるいは少なくともｆ（x_2））に、公開署名ｐに対応する秘密の署名鍵を使って署名を行い、Ｅとｆ（x_2）と署名を銀行３０に送る。任意で売り主２０はさらに、前述したような方法、すなわち銀行の暗号鍵あるいは付随的な相対鍵を使って、このメッセージを暗号化してもよい。

銀行３０は、自身の秘密鍵を使って売り主２０からのメッセージを解読した後

、x_1がすでに保存されていないかデータベースを調べ、もし見つからなかった場合には、銀行３０はx_1を保存する。さらに銀行３０は、ｆ（x_1）に関連した値に等しい額を売り主２０に振替えるという内容が記載されたノートＣ（ｆ（x_2））を生成する。前記ノートは売り主２０に送られ、領収書発行と確認が済んだ後、購入された品物は顧客１０に送られる。

実質的に、暗号化された最後のプロトコルは前述のものとほぼ同じである。暗号化が加えられたのは、支払人が受取人経由で「為替」を渡す処理においてであり、その間支払人の与えた秘密や付加情報は、中身がいたずらされていないことは保証される。

ノートＣ（ｆ（x_1））に処理が完了した日付を入れておくことは有益なことである。この場合、銀行３０のデータベースに保存されているx_1はさほど大きくならない。これは、x_1を銀行のデータベースに永遠に保存しておく必要がないことによる。電子通貨の価値が失効しないように、スマートカード（あるいは顧客が取り引きをするために操作する装備すべて）は、自動的に古くなった電子通貨を新たな有効期限を持った新しい電子通貨に更新する。

満了日まで、電子通貨の払い戻しはできる。スマートカードの期限が過ぎて、全てのｘ１を失っていしまった場合、期限満了後３ヶ月以内に申し立てておらず、ユーザが電子通貨の価値に相当する額の信用貸しの要求を、銀行３０にｆ（x_1）と共にすることができる。しかしながら、一連のこの処理では、銀行との間で最初の通信であり、この場合には貨幣の引き出しを行っているときに、顧客１０は、自分自身であることを証明する。

プロトコルの顧客側は、x_1だけを保存すればよいので、スマートカードを使って簡単に装備することができる。また、一般的には、顧客は多くの金を必要としない。スマートカードを盗んだ者にx_1の値を盗まれないようにするため、ＰＩＮが極秘にスマートカードに使われていて、x_1をアクセスする前にユーザが入力しなければならない。

以上記載した相互作用はすべて自動的に行われているのは当然のことであることに、注目してほしい。これらの処理は、適切なプログラムがされたコンピュー

タやプロセッサによって自動的に実行される。　コンピュータやプロセッサは、取り引きを行う関係者によって実装され、その管理下にある。

その他の実施例は、以下に記載する。例として、秘密の値x_1を使って電子通貨と認証情報を結合するためのその他の手法がある。これもまでの記載では、秘密の値ｘ１は電子通貨を発行する人によって任意に生成されると仮定していた。しかしながら秘密の値は、一方向関数ｈ（ｘ）を用いて何らかの認証データのイメージを生成してもよい。この一方向関数は、あるいは通常の電子通貨の組み立てに使われる関数ｆ（ｘ）と同じであってもよい。認証情報は、用途、支払日、支払人の名前、予定の受取人といったもの、まとめていえば、支払人が銀行に（保管しておきたいと思っているすべての情報、を含む。これらの情報は、ｈ（ｘ）を通して、秘密の値となるx_1を生成する。

この場合銀行は、前述の「ドロップ」あるいは「電子為替」プロトコルで行われた電子支払いで受信した取り引き情報を保存する必要はなくなる。本質的には、求められていることの全ては、払い込みが要求に応じて受取人を匿名にしないでラベル付けが行われることである。銀行が積極的に受取人の識別を行い、受取人のＩＤを含む取り引きの標準記録を保管していれば、支払人は後できちんと支払ったことを、ｆ（ｘ）に用いたx_1のプレイメージを公に明らかにすることによっ

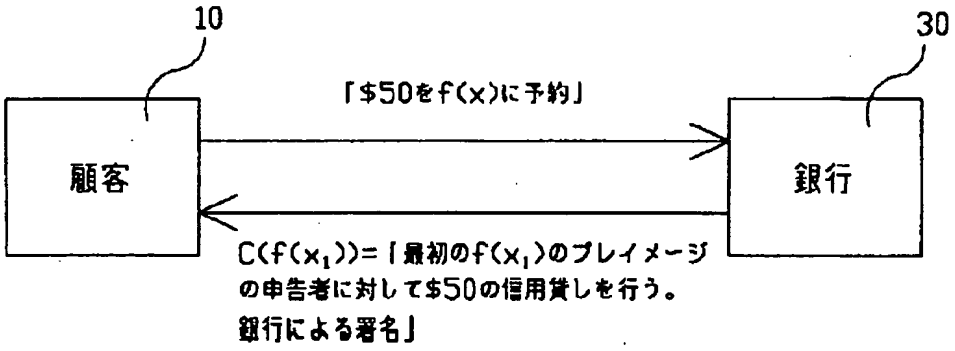
て立証することができる。なぜなら、前記情報を示すｆ（ｘ）は、用途や支払日、支払人の名前、予定の受取人といった情報を含んでいるからである。x_1の値として普通に結合し、さらに他の電子通貨と交換して運ばれた暗黙の情報を、支払人は電子通貨と一緒に手に入れることができる。しかしながらこのような状況では、払い込み情報は暗黙のうちにx_1に含まれているため、銀行に送る必要ない。それゆえ、支払人が安全のため銀行を通過させなければならない情報は、受取人の認証に使われる公開署名鍵だけである。この情報は、暗黙のうちに支払人の要求で名前を明かして通信が行われる。

署名を基本とした通信を要求しているが、実際には、情報がx_1（あるいは$f(x_1)$）とぴったりと一致していなければ、銀行は名前を明かして電子通貨を

引き受けることはできないので、受取人の身元の確認は排除される。例として、いくつかのx_1の特性（例えば、第１ビットが１であった場合）、銀行によって問題の電子通貨は名前を明らかにした場合のみ取り扱うという表明として公に宣言される。支払人は、ｆ（s_j）によって秘密のx_1を算出することができる。s_jは、特定の取引の情報と任意の値ｒを結合したものであり、その結果、x_1は非匿名性を持つことになる。このような性質のうち、およそ半分は、プレイメージs_jをｆ（ｓ）で演算し、その結果として得られたある特定のデータ長を持つｆ（s_j）によって決まるので、所望の効果を持つx_1を見つけるまで、何回化のｒを選ばなければならない。このような電子通貨は、これを回収しようとする者は自身のＩＤを提供し、かつ銀行が納得するようにその証明をしなければならない、という性質を持つ。このため、銀行は通常の取引情報の一部として交換を申し出た者のＩＤを記録しておくことができる。この結果、この電子通貨を作成した者は、後にその起源と同様、その他の取り引きの詳細（起用予定も含めて）をも、銀行の取り引き記録を参照し、ｘｉを生成するのに用いられるs_jを明らかにすることによって立証することができる。それゆえ、電子通貨を、余分の暗号や銀行に対しの情報を付加せずにまったく普通に使ったとしても、支払人には前述した「電子為替」によって必要な防護機能すべてが提供される。

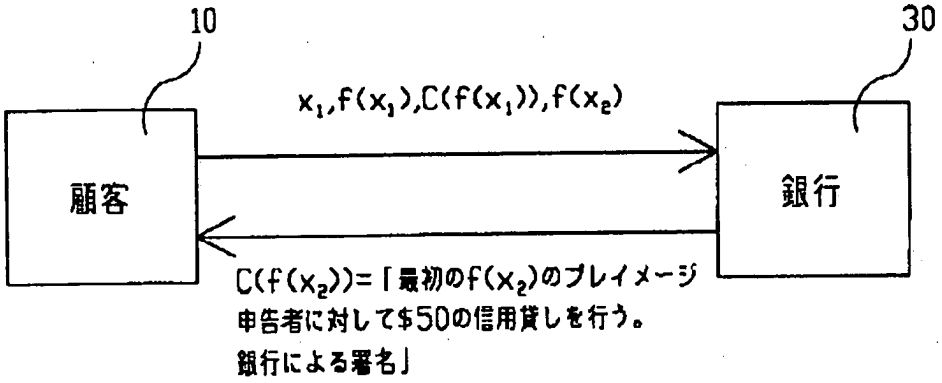
【図１】

図1



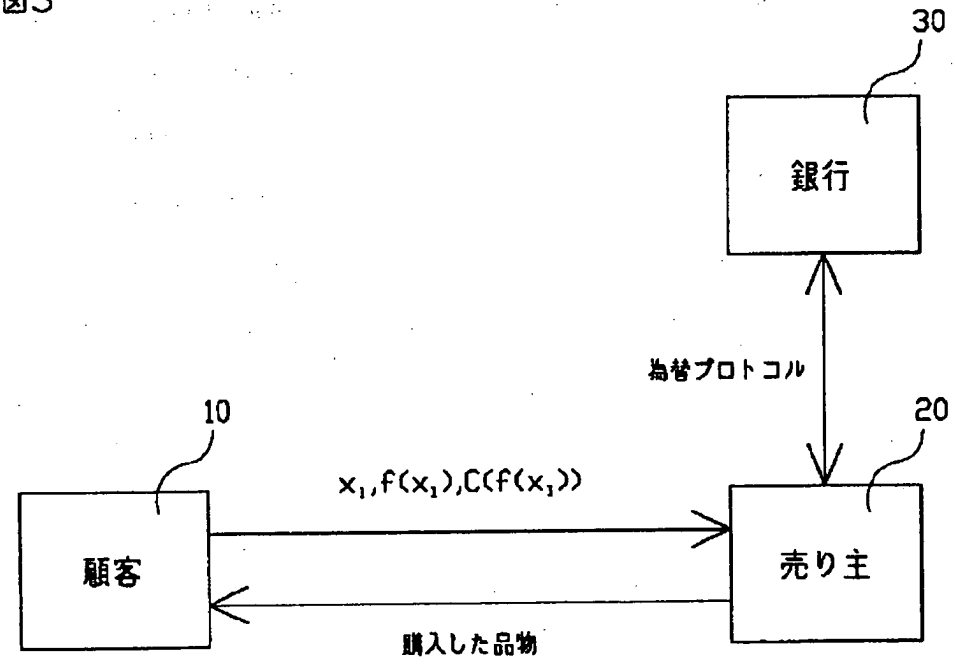
【図２】

図2


10
30
$x_1, f(x_1), C(f(x_1)), f(x_2)$
顧客
銀行
$C(f(x_2))$=「最初の$f(x_2)$のプレイメージ
申告者に対して$50の信用貸しを行う。
銀行による署名」

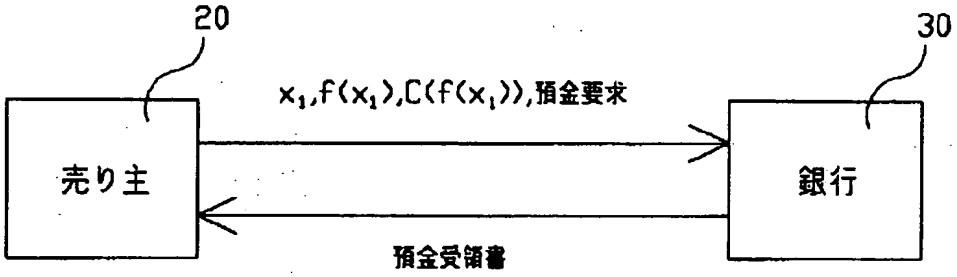
【図３】

図3


30
銀行
為替プロトコル
10
20
$x_1, f(x_1), C(f(x_1))$
顧客
売り主
購入した品物

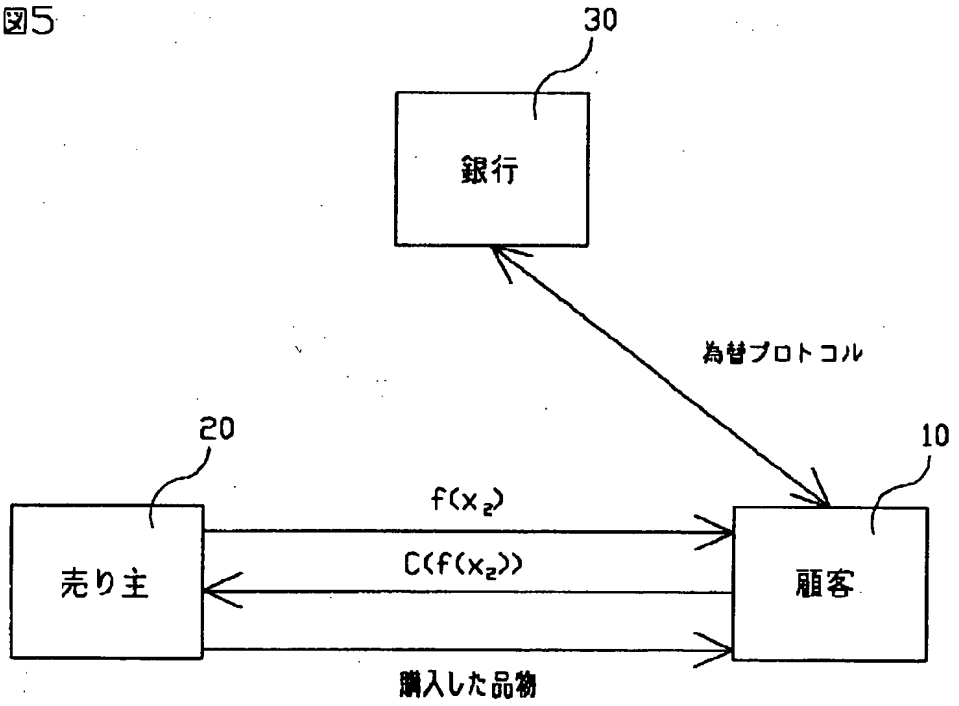
【図４】

図4


20
30
$x_1, f(x_1), C(f(x_1))$, 預金要求
売り主
銀行
預金受領書

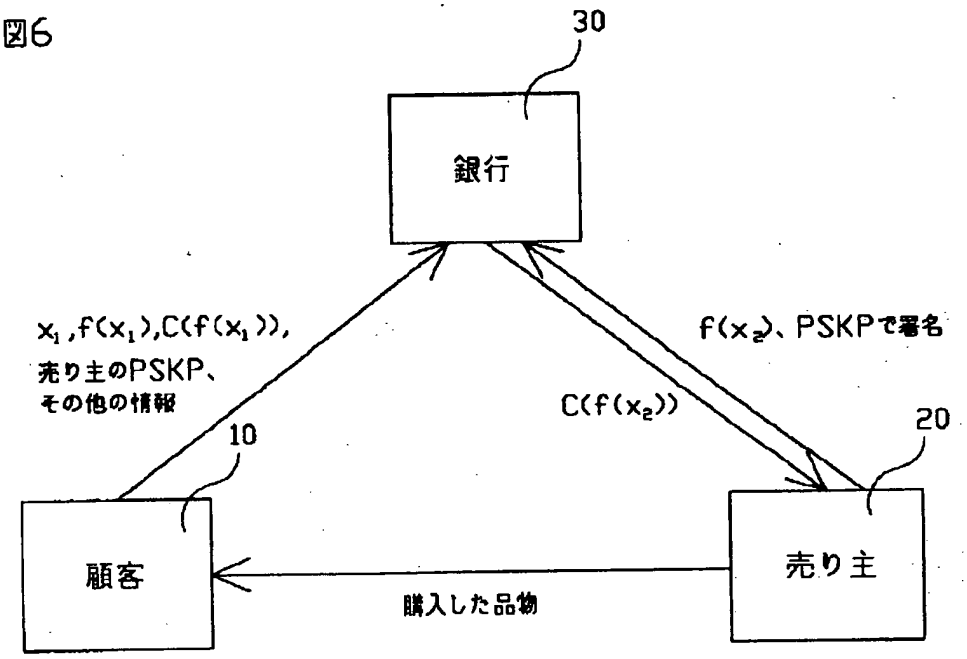
【図５】

図5


30
銀行
為替プロトコル
20
10
$f(x_2)$
$C(f(x_2))$
売り主
顧客
購入した品物

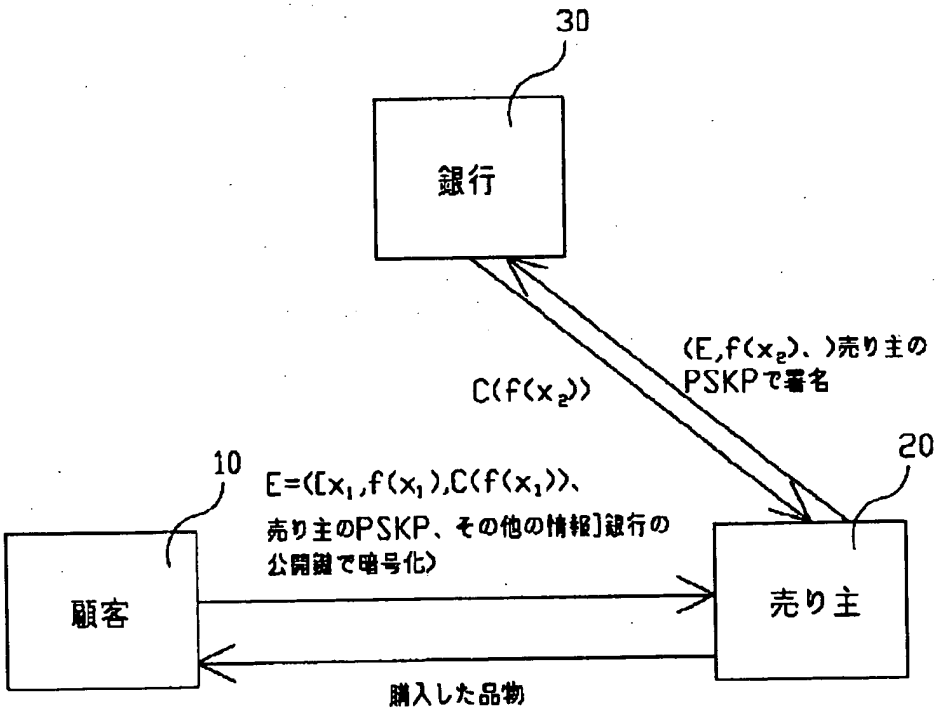
【図６】

図6


30
銀行
x_1 ,$f(x_1)$,$C(f(x_1))$,
売り主のPSKP、
その他の情報
$f(x_2)$、PSKPで署名
$C(f(x_2))$
10
20
顧客
売り主
購入した品物

【図７】

図7


30
銀行
(E,$f(x_2)$、)売り主の
PSKPで署名
$C(f(x_2))$
10
20
$E=([x_1,f(x_1),C(f(x_1))$、
売り主のPSKP、その他の情報]銀行の
公開鍵で暗号化)
顧客
売り主
購入した品物

【手続補正書】特許法第１８４条の８第１項

【提出日】１９９７年９月４日（１９９７．９．４）

【補正内容】

明細書

追跡不可能な電子通貨システム

背景技術

この発明は、電子通貨システム一般に関する。

電子通貨システムの直観的にわかる最終的な形態は、有形の現金の最良の特徴（プライバシーが守られる、匿名性、偽造しにくい）と、電子取り引きの持つ最良の特徴（速さ、簡便性、輸送や保管に対する潜在的な安全性）を合わせ持った形態である。匿名性を有す電子通貨システムを実現するための基本的な問題は、次のように単純化することができる。２つの連続した取り引きにおいて、この電子通貨の所有者が識別できなかったならば、この所有者が第一の取り引きがなかったように振る舞い、同じ電子コインを再び使用することをどうやって防ぐかという問題である。この問題に対する第一の解決方法は、チャーム、フィアットとノアーによって提案されている（Ｄ．チャーム(D.Chaum)、Ａ．フィアット(A.Fiat)、Ｍ．ノアー(M.Noar)著、アントレーサブル・エレクトロニック・キャッシュ(Untracedable Electronic Cash)、Proc. CRYPTO'88、Springcr-Verlag(1990)、319-327ページ）。これは、同じ電子通貨が２回、中央の銀行に送られてきた場合には、通貨の二重使用を検出して二重使用を行った人の特定が十分に行えるということを前提条件として成立している。他の解決方法の提案のうちのいくつかにもこの前提が用いられていて、銀行は各取り引きを複雑にする必要がないという利点を有す。しかしながら実際には、この前提条件には重大な欠点がある。それは不正な取り引きは発生後しばらくたってから検出されるということであり、不正実行者が法によって処罰されないという確信があれば（アクセスできない状態であったり、第三者のＩＤや電子通貨を使っている場合など）、不正実行者は意のままに電子通貨の二重使用をすることができる。

概して、この発明には２つの簡単な基本要素である、一方向関数と署名機構を用

いている。どちらもよく知られた技術であって、詳細については、一般に入手できる暗号に関する本で知ることができる。例えば、ブルース・シュネイヤー（Bruce Schneier）著、アプライド・クリプトグラフィー（Applied Cryptography）（１９９４年　ジョン・ウィリー・アンド・サンズ社（John Wilcy & Sons, Inc.）刊にある。このシステムは、電子通貨を使う人の匿名性を保護することはもちろん電子通貨の正当性を保証するものであるばかりでなく、偽造することはできず、また１回しか使用できない。

本発明の一形態である電子通貨プロトコルは、一方向関数f_1（x）を用いて変換前の元の値であるプレイメージx_1から変換後の値であるイメージf_1（x_1）を生成する手順、イメージf_1（x_1）を目隠ししない形式で第二の当事者に送信する手順、第二の当事者からディジタル署名を含む文書を受け取る手順とから成る。前記受け取った署名を含む文書は、第二の当事者が、第一のプレイメージx_1を決めた者に対してあらかじめ決められた金額を信用貸しするという確約を意味する。

本発明の最良の形態は、次に示すような形態を含む。本発明の電子通貨プロトコルはまた、第三の当事者から購入した商品や受けたサービスに対する支払いとして、プレイメージx_1を第三の当事者へ送る場合も含んでいる。またさらに、第二のプレイメージx_2を選択し、第二の一方向関数f_2（x）により第二のプレイメージx_2を第二のイメージf_2（x_2）に変換し、第一のプレイメージx_1と目隠ししない形式で第二のイメージf_2（X_2）を第二の当事者に送信し、第二の当事者からディジタル署名を含む文書を受信するという形態もある。前記文書は、第二の当事者が、第一のプレイメージx_2を決めた者に対してあらかじめ決められた金額を信用貸しするという確約を意味する。どちらの場合も、f_1（x）とf_2（x）は同じ関数である。後者の場合、第二の当事者に対して第一のプレイメージx_1と目隠ししない形式で第二のイメージf_2（X_2）を送信しているのは、匿名性を保持するためであり、第二の当事者は銀行である。

また、本発明の最良の形態であるプロトコルには、第三の当事者の署名鍵と第一のプレイメージx_1を結合して情報をひとつのブロックに構成する手順、前記

情報ブロックを第二の当事者の暗号鍵を使って暗号化して、暗号化された情報ブロックとする手順、前記暗号化された情報ブロックを第三の当事者に送信する手順とから成るものかある。

その他の形態である本発明の電子通貨プロトコルは次の手順で行われる。まず第一の当事者から第一のプレイメージx_1を受け取る手順であり、このプレイメージx_1は第一の一方向関数$f_1(x)$によって処理され第一のイメージ$f_1(x_1)$となる。前記第一のプレイメージx_1は、第二の当事者が前記第一のプレイメージx_1を第二の当事者に申告した第一の当事者に対して、予定額の信用貸しを行うという、第二の当事者による確約と連結している。さらに、第二のプレイメージx_2を選択する手順、第二の一方向関数$f_2(x)$により第二のプレイメージx_2から第二のイメージ$f_2(x_2)$を生成する手順、第一のプレイメージx_1と目隠しされない形式の第二のイメージ$f_2(x_2)$を第二の当事者に送信する手順、第二の当事者からディジタル署名を含むノートを受信する手順とから成る。このノートは、第二のプレイメージx_2を第二の当事者に送った第一の当事者に対し、予定の額の信用貸しを行うという第二の当事者の約束を表わしている。

さらなる他の形態では、本発明の電子通貨プロトコルは次の手順で行われる。まず、第一の当事者から暗号化された情報のブロックを受け取る手順であり、この情報が暗号化されたブロックは、第二の当事者の公開署名鍵と第一のプレイメージx_1とを連結して情報のブロックが構成され、さらに前記情報のブロックは第三者の暗号鍵を使って暗号化されたものである。

第６図は、匿名あるいは匿名でないドロップ・ペイメントまたは為替プロトコルを示す図である。第７図は、暗号化した為替プロトコルを示す図である。

発明を実施するための最良の形態

匿名で通信する能力は、いろいろな意味で、匿名の金銭取り引きが行われる場合には優先されなければならない事項である。なぜなら、ある団体の通信についての情報は、その団体の商取り引きに関する情報を明らかにしてしまうからである。実際には、通信の匿名性が基礎としているのは、電話会社が自社のシステムの秘密性を保護しているという信頼にすぎない。各団体は正体のわからない匿名

での返信者を信頼するか、あるいは文献から公に入手できる他の技術のひとつを装備して信頼するかの選択ができる。

団体間の通信は第三者に対して匿名性を持つばかりでなく、その団体間でも互いに匿名性を持って通信を行うことを想定する。（代表的な実施例において、後者の形態は自己認識を除いて前者の自然な結果である。）このような条件における、簡単で幾分匿名性を有す電子通貨システムのプロトコルを第１図に示す。

以下で説明するさまざまなプロトコル（第１図から第７図を参照のこと）では、３団体を顧客１０と売り主２０と銀行３０という名称で定義する。顧客１０は、もちろん一般的には支払人の代表であり、売り主２０は一般的には受取人の代表である。当然ではあるが、この設定は説明を明快にする目的で決めたもので、この発明の範囲を限定するものではない。従って当然ながら、この三者を集団Ａ、集団Ｂ、集団Ｃとして引用しても同じ効力を持つ。

図には、いくつかの異なった団体がブロックによって示されており、ある団体から他の団体への情報の伝達は該当するブロックをつなぐ線によって示している。各線は、ある団体から他の集団へ一定の情報が伝わることを示しており、線の端の矢印が通信の方向を示している。伝達される情報は、内容をまとめたシンボルとして、線の下に示してある。

各ブロックにはラベルか付けられ、次に示すような特定の物として記述されているか、前記特定の物による処理は、コンピュータ処理や通信を実行するコンピュータ機器によって実行されるものである。コンピュータ機器は、多岐にわたる種類の電子機器を含んでいる。例えば、パーソナル・コンピュータ、ＰＣカード（ＰＣＭＣＩＡ対応カード）、ＰＤＩ、スマートカード、パームトップコンピュータ、強力なワークステイション等でありこれらはその一部に過ぎない。次に説明するように、プロトコルの銀行側の処理は、現在ＡＴＭによるトランザクションを処理しているサーバと同様に、電子商取引を処理するようにプログラムされたサーバによって実行される。前記サーバは、データの到着する複数の電話線を有し、関連データを保存するためのデータ記憶容量を持っていることが望ましい。

コンピュータ機器が内部あるいは外部に、プロトコルを実行するするために必要なプログラムやデータのために必要なメモリを有していることは当然のことである。さらに、前記コンピュータ機器は、例えばモデムのような、他のコンピュータ機器と通信を行うための手段も有す。さらに付け加えれば、情報を伝送する通信媒体は非常に多くの可能性を持っている。媒体の例としては、電話線、ケーブル、インターネット、衛星通信、無線通信などが挙げられる。言い換えれば、本発明は、使われている機器の種類や採用している通信方法によって限定されるものではない。可能性や組み合わせは、人の創作力によって限定されるものである。

これから説明するプロトコルにおいては、銀行３０が公に使用できる一方向関数ｆ（ｘ）を、選択し、制定する。このような関数は、誰もが商取引においてアクセスし使うことができるように、誰でもが公に入手できるものでなくてはならない。一般に、一方向関数は、X_1を使ってｆ（x_1）を算出することはできるが、ｆ（x_1）を与えられてもx_1を算出できない関数ｆ（ｘ）を意味する。以下の説明では、x_1はｆ（x_1）のプレイメージと、ｆ（x_1）はx_1のイメージとする。

実際には、完全な一方向関数は存在しない。現在一方向関数と考えられているすべての関数は、コンピュータの能力や手法によってｆ（x_1）からx_1を決定することか十分にできる。それゆえ、一方向関数という語には、ｆ（x_1）からx_1を算出することが、不可能である必要はないが非常に難しい関数であるという意味も含まれる。

一方向関数は、標準のハッシュ関数（例えば、ＭＤ５、ＳＨＡ等）のうちのいずれかでよい。さらにつけ加えれば、いくつかの一方向関数を使うことも、これを結合することも可能である。この技術分野において、多くの一方向関数が知られている。その中の幾つかは、コンピュータに移植することが簡単で、スマートカードに装備することもできる。

以上の基礎知識を前提として、本発明の実施の形態となる種々のプロトコルについて説明する。まず、顧客が銀行から「キャッシュ」を手に入れる処理に用い

られる電子通貨の引き出しプロトコルから始める。

引き出しプロトコル

電子通貨の引き出し処理は、第１図に示した手法に従って行われる。顧客１０は、任意の数x_1を選び、一方向関数ｆ（ｘ）を使って変換後の値であるx_1のイメージを生成する。x_1の値は後処理装置が任意で行っているような乱数発生手段から得られた無作為の数列である。この数列は、例えば１２８ビット長のデータである。顧客１０は、支払い処理が発生してから完了するまでx_1の値を秘密にしておく。

顧客１０は、金額とｆ（x_1）をまとめて銀行３０に送って引き出しの要求を行い、銀行３０から金を引き出す（匿名ではなく）。銀行３０は、明細書にディジタル署名を行って顧客の趣意に従う。このようにｆ（x_1）を正規の電子通貨として認定し、要求の額を、顧客１０が銀行３０に持っている口座の借方に記入する。言い換えれば、銀行３０は、「最初にｆ（x_1）のプレイメージを決めた者に対して、総額ｚの信用貸しを行う」ことに関して銀行３０は署名を行って証明する、という効力を表わす明細書あるいは覚え書きを発行する。

署名や情報の認証を行う技術（例えば、秘密鍵と公開鍵のペアを使う方法）や、ディジタル署名の手法は、よく知られている技術である。さらに詳しくは、この分野において広く認められた参考文献を参照すればよい。例えば、ブルース・シュネイヤー(Bruce Schneier)著、アプライド・クリプトグラフィー(Applied Cryptography)、１９９４年　ジョンウイリー・アンド・サンズ社(JohnWilcy&Sons,Inc.)

などである。

一般的に署名機構とは、文字にタグを付けるやり方のことである。典型的な例としては、公開鍵と秘密鍵のペアを使うものがある。公開鍵及び秘密鍵は、一方向関数を使って実行される。より現実的なアプローチ方法としては、さらに効果を上げるためにトラップ・ドア機能を使う方法がある（例えば、スキネイナー(Schneiner)著、ＲＳＡ、ＤＳＳ、エルガマ・アルゴリズム(RSA, DSS, Elgamal algorithms)参照のこと）。秘密鍵は、文字か文字列のいずれかを暗号化するのに

使われ、文字に添付するディジタル署名として使われる。ディジタル署名は、自身の秘密鍵を持っている者の署名であることを示している。なぜなら、他者が前記文字列からこのような署名を作り出すことはできないからである。第二の当事者が公開鍵を使ってタグの暗号を解読すれば、署名者自身の秘密鍵によって署名がなされたことがわかる。この手法を保証するために、署名をした人の公開鍵を誰もが手に入れまた預けられてこと、かつ秘密鍵は危険にさらされることはないと信頼できることが、前提となっていることは明らかである。

公開鍵を公表すること、及び銀行３０が第一のｆ（x_1）のプレイメージを決めた者に対して明記された額を支払うという覚え書きにディジタル署名を添付したことにより、銀行３０はその責任を明らかにし、さらに偽造者から自身を守る。

銀行が発行した、証明書となる覚え書きをここではＣ（ｆ（x_1））と定義し、ノートと呼ぶ。このノートは顧客１０に返送される。さらに付け加えれば、ノートは公然と入手することができるが、x_1を知らない人にとっては何の価値もない。

交換プロトコル

関係者（例えば、顧客１０や売り主２０）は、いつでも、銀行３０において匿名で電子通貨の「交換」ができる。実際には、相手側当事者から電子通貨を受け取ったら、処理を迅速に行うことが特に重要である。これは、電子通貨の正当な受取人の前に誰か他の者がx_1を銀行３０に送信してしまうリスクを最小にするためである。不正実行者は、複数の者に対してx_1を送信し、その電子通貨を複数回、送信しようとするかもしれない。そのようなことが起きたら、銀行３０に届いた最初の受取人がその価値を受け取り、その他の電子通貨の受取人達は該当しない電子通貨となり交換することができない。売り主２０にとっては、交換のタイミングはさほと重要でない。なぜなら、大体において売り主２０は、電子通貨の受け取りが有効に完了するまでは、納入予定の品物やサービスを提供しないからである。　第２図に示したように、顧客１０が電子通貨を匿名で交換することを望んだと仮定すると、顧客１０は銀行３０にx_1と任意に選ばれたx_2の変換

後のイメージである f （x_2）を送信する。言い換えれば、顧客１０は x_1によって前述したような引き出しプロトコルを行い、同時に引き出した総額を提供する。銀行３０は単に f （x_2）を認証し、f （x_1）は「すでに使われた」ということの証明として x_1をデータベース４０に保存するだけである。これが x_1の二重使用されるのを防止する交換の手法である。

f （x_1）とC（f （x_1））はすでに銀行３０が所有しているので、銀行３０に対して x_1と f （x_2）といっしょにその情報を送ることは任意である。

プロトコルの銀行側処理がサーバーに実装されていれば、銀行は受信した x_1を自動的に保存する。さらに、銀行３０がもうひとつの x_1を受け取る毎に、最初にそれがすでに使われたもの(すなわち受信されたもの)であるかをチェックする。

誰が実際に電子通貨を使っているのかがはっきりわからない交換処理を、連続して取り扱うことができるようになる。交換処理には f （x_2）を明らかにすることのみが必要であり、x_2の持ち主を明らかにする必要はないことに注目してほしい。匿名を実現するための他の手法と違って、電子通貨を目隠しすること等その他の処理を必要としない。実際には、f （x_1）が目隠しされず、広く一般に知られていることが望ましい。

通信の匿名性を確保するよう求める手法は何でも、処理の匿名性が確保されれば十分に目的を果たす（すなわち、匿名性を実現することは可能であるが必須ではない）。

この手法は、電子通貨を両替する方法として使うこともできる。f （x_2）を

送信する代わりに、

信用取引が登録されたことを確認するために預金の受領書を売り主２０に送る。

プロトコルの拡張

以上説明した電子通貨手法における交換及び支払プロトコルには、いくつかの他の実施の形態の例がある。これら他の実施の形態は、求められている匿名性のレベルや関係に応じた有効な手段となるように作られている。例えば、第５図に

示したのは、顧客１０が売り主２０よりも銀行３０にアクセスするほうが容易である場合、売り主２０は最初に顧客１０にｆ（x_2）を送り、顧客１０は売り主２０の代わりに交換プロトコルを行い、支払いの証明として署名された電子通貨、例えばＣ（ｆ（x_2））を返送する。前述したように、交換プロトコルは匿名で行われる。

あるいは、顧客１０及び売り主２０の双方が、お互いよりも銀行とよい関係をもっている場合、図６に示したような「ドロップ」ペイメントプロトコルを使うとよい。このプロトコルに従えば、顧客１０は売り主２０のための支払いを銀行に降ろし、売り主２０はその後すぐに銀行から支払いを回収する。

「ドロップ」支払いプロトコルの手順を以下に示す。最初に、顧客１０がある特定の額の貨幣の代わりとしてのx_1を銀行３０に送る。この時、売り主２０の公開署名鍵ｐ（ＰＳＫＰ）と取り引きに関する情報を付加して送る。いろいろな情報があるが、例えば、顧客１０が購入した品物を明らかにしたり取り引きを確認することを望んだ場合、さらに/あるいは売り主が支払いに関する顧客の意向を認めたといことを指示する場合などがあり、その結果、電子通貨が本質的な意味において、「電子為替」に変る。顧客１０は任意でｆ（x_1）とノートＣ（ｆ（x_1））を送ってもよいが、前述したように、この情報はすでに銀行３０が入手しているので、送る必要はない。

顧客１０が提供したその他の情報から集められた記録は、遠隔支払設定として特定の用途に使えるかもしれない。取り引きの性格が特に暗黙であるという場合でなければ、典型的には個人的な支払い方法になる。

もし、売り主２０が匿名性を保持することを望まなければ、公開署名鍵は売り主２０のＩＤと明らかに関係しているものであってよいが、もし匿名性を望むのであれば、公開署名鍵はＩＤとはまったく関係ない特別な目的を有した公開鍵としなければならない。後者の場合には、公開鍵は信頼できる知人に極秘に渡すか、単純に匿名で公表する。

銀行３０はx_1に付随した第一の電子通貨ｆ（x_1）として表わされた総額を渡すことに同意し、以前に配布された公開署名鍵ｐと対応する秘密の署名鍵を使っ

て署名されている。このようにして、顧客１０が購入しようとした品物の支払いを手に入れるために、売り主２０は、第１図に関連して以前に記述したプロトコルを使って、銀行３０から金を引き出す。このとき、売り主２０は任意のx2を選択し、f（x）を使ってイメージf（x2）を生成する。しかしながらこの例では、売り主２０はf（x2）を銀行３０に送信する前に秘密署名鍵を使ってf（x2）に署名を行う。付け加えると、この場合、貨幣は売り主の口座から引き出されるのでなく、顧客１０によってこの処理の前に与えられた口座から転送するだけである。

銀行３０は売り主の公開署名鍵を使って、受信したf（x2）が売り主２０（すなわち貨幣の転送を行った者）によって署名されことを確かめる。f（x2）の署名を確認すると、銀行３０は売り主２０に送信するノートCf（x2））を発行する。

金を受け取ったという確認のノートC（f（x2））を売り主２０が受け取った後、売り主２０は顧客１０に品物を送る。

もちろん理論上は、銀行３０は支払先に金を与える代わりに金を自分のものにすることによってだますことができる。しかしながら、支払人の匿名性を信頼している、あるいは少なくとも一般の人々が銀行３０が不正しないことをモニターしているので、支払人が取り引きを暴露する可能性をあてにすることができる。

関係者間の通信が傍受されているという設定のもとで、交換プロトコルを安全なものにする、とりわけ秘密のxの値をが立ち聞きする者を通り抜けて通過するいくつかの方法がある。最も自然な方法は、公開鍵による暗号法である。関係者が銀行のものはもちろんのこと互いの公開暗号鍵を知っていれば、銀行３０が送信するものを除くすべてのメッセージが、受信側の公開暗号鍵を使って暗号化するか、受信側の公開暗号鍵を使って暗号化された相称的な「セッションキー」を使っているかぎり、前述した全てのプロトコルが立ち聞きするものを絶滅させるように機能する。もちろん銀行のメッセージは、秘密でなくてよいよう考慮されている。なぜならメッセージは、xiが誰か他の者によって秘密にされているf（xi）という形式の署名された貨幣だけで構成されているからである。暗号化

処理時にメッセージの認証コードやＭＡＣを使えば、メッセージが目的地に到着するまで送り主以外の誰かによっていたずらされることはないことが保証される。

公開暗号鍵の使用により、別の種類の「電子為替」が可能となる。この事例を第７図に示し、暗号化された電子為替プロトコルとして一般にあてはめる。顧客１０は、ある正規の電子通貨としての秘密のｘｉの値を、売り主２０の公開鍵ｐとその他の必要なＩＤや取引情報といっしよに暗号化する。前述の「ドロップ」プロトコルの場合と同様である。顧客１０はこの情報を、銀行の公開暗号鍵を使うか、あるいは銀行の公開暗号鍵を使って暗号化されたセッションキーを使って暗号化する。その後、顧客１０は暗号化された情報を直接売り主２０に送信する。

これを「現金」にするために、売り主２０は任意の値x_2を選び、そのイメージｆ（x_2）を生成し、顧客１０から受信したメッセージＥにｆ（x_2）を添付する。前と同様、ｆ（x_2）は銀行によって署名されると、それは売り主２０への金の移転を意味する。売り主２０は完了メッセージ（あるいは少なくともｆ（x_2））に、公開署名ｐに対応する秘密の署名鍵を使って署名を行い、Ｅとｆ（x_2）と署名を銀行３０に送る。任意で売り主２０はさらに、前述したような方法、すなわち銀行の暗号鍵あるいは付随的な相対鍵を使って、このメッセージを暗号化してもよい。

銀行３０は、自身の秘密鍵を使って売り主２０からのメッセージを解読した後、x_1がすでに保存されていないかデータベースを調べ、もし見つからなかった場合には、銀行３０はx_1を保存する。さらに銀行３０は、ｆ（x_1）に関連した値に等しい額を売り主２０に振替えるという内容か記載されたノートＣ(ｆ(x_2))を生成する。前記ノートは売り主２０に送られ、領収書発行と確認が済んだ後、

購入された品物は顧客１０に送られる。

実質的に、暗号化された最後のプロトコルは前述のものとほぼ同じである。暗号化が加えられたのは、支払人が受取人経由で「為替」を渡す処理においてであ

り、その間支払人の与えた秘密や付加情報は、中身がいたずらされていないことは保証される。

ノートＣ（ｆ（x_1））に処理が完了した日付を入れておくことは有益なことである。この場合、銀行３０のデータベースに保存されているx_1はさほど大きくならない。これは、x_1を銀行のデータベースに永遠に保存しておく必要がないことによる。電子通貨の価値が失効しないように、スマートカード（あるいは顧客が取り引きをするために操作する装備すべて）は、自動的に古くなった電子通貨を新たな有効期限を持った新しい電子通貨に更新する。

満了日まで、電子通貨の払い戻しはできる。スマートカードの期限が過ぎて、全てのx_1を失っていしまった場合、期限満了後３ケ月以内に申し立てておらず、ユーザすなわち顧客１０が電子通貨の価値に相当する額の信用貸しの要求を、銀行３０にｆ（ｘｉ）と共にすることができる。しかしながら、一連のこの処理では、銀行との間で最初の通信であり、この場合には貨幣の引き出しを行っているときに、顧客１０は、自分自身であることを証明する。

プロトコルの顧客側は、x_1だけを保存すればよいので、スマートカードを使って簡単に装備することができる。また、一般的には、顧客は多くの金を必要としない。スマートカードを盗んだ者にx_1の値を盗まれないようにするため、ＰＩＮが極秘にスマートカードに使われていて、x_1をアクセスする前にユーザが入力しなければならない。

以上記載した相互作用はすべて自動的に行われているのは当然のことであることに、注目してほしい。これらの処理は、適切なプログラムがされたコンピュータやプロセッサによって自動的に実行される。　コンピュータやプロセッサは、取り引きを行う関係者によって実装され、その管理下にある。

その他の実施例は、以下に記載する。例として、秘密の値x_1を使って電子通貨と認証情報を結合するためのその他の手法がある。これもまでの記載では、秘密の値x_1は電子通貨を発行する人によって任意に生成されると仮定していた。しかしながら秘密の値は、一方向関数ｈ（ｘ）を用いて何らかの認証データのイメージを生成してもよい。この一方向関数は、あるいは通常の電子通貨の組み立

てに使われる関数ｆ（ｘ）と同じであってもよい。認証情報は、用途、支払日、支払人の名前、予定の受取人といったもの、まとめていえば、支払人が銀行に保管しておきたいと思っているすべての情報、を含む。これらの情報は、ｈ（ｘ）を通して、秘密の値となるx_1を生成する。

この場合銀行は、前述の「ドロップ」あるいは「電子為替」プロトコルで行われた電子支払いで受信した取り引き情報を保存する必要はなくなる。本質的には、求められていることの全ては、払い込みが要求に応じて受取人を匿名にしないでラベル付けが行われることである。銀行が積極的に受取人の識別を行い、受取人のＩＤを含む取り引きの標準記録を保管していれば、支払人は後できちんと支払ったことを、ｆ（ｘ）に用いたx_1のプレイメージを公に明らかにすることによって立証することができる。なぜなら、前記情報を示すｆ（ｘ）は、用途や支払日、支払人の名前、予定の受取人といった情報を含んでいるからである。x_1の値として普通に結合し、さらに他の電子通貨と交換して運ばれた暗黙の情報を、支払人は電子通貨と一緒に手に入れることができる。しかしながらこのような状況では、払い込み情報は暗黙のうちにx_1に含まれているため、銀行に送る必要なない。それゆえ、支払人が安全のため銀行を通過させなければならない情報は、受取人の認証に使われる公開署名鍵だけである。この情報は、暗黙のうちに支払人の要求で名前を明かして通信が行われる。

署名を基本とした通信を要求しているが、実際には、情報がx_i（あるいは$f(x_i)$）とぴったりと一致していなければ、銀行は名前を明かして電子通貨を引き受けることはできないという趣旨により、受取人の身元の確認は排除される。

請求の範囲

１．電子通貨システムの実施手法であって、

一方向関数f_1（ｘ）を用いて演算前の元の値であるプレイメージx_1から演算後であるイメージ$f_1(x_1)$を生成する手順、

イメージ$f_1(x_1)$を見える形式で第二の当事者に送信する手順、

前記第二の当事者からディジタル署名を含む文書を受信する手順、

から成り、

前記文書が前記第二の当事者があらかじめ決められた金額を第二の当事者に対応するプレイメージx_1の申告者に信用貸しするという確約を表すことを特徴とする電子通貨システムの実施手法。

２．第三の当事者からの商品の購入及び第三の当事者からのサービスに対する支払いとして前記プレイメージを第三の当事者へ送信する手段をさらに有することを特徴とする請求の範囲１に記載の電子通貨システムの実施手法。

３．請求の範囲１に記載の電子通貨システムの実施方法に加えて、

第二のプレイメージx_2を選択する手順、

第二の一方向関数f_2（ｘ）を用いて第二のプレイメージx_2からイメージf_2（x_2）を生成する手順、

第一のプレイメージx_1と目隠しされない形式のイメージf_2（x_2）を第二の当事者に送信する手順、

前記第二の当事者からディジタル署名を含む第二の文書を受信する手順、

から成り、

前記第二の文書が前記第二の当事者があらかじめ決められた金額を前記プレイメージx_2を第二の当事者に申告した者の貸し方に記入する確約を意味することを特徴とする電子通貨システムの実施手法。

４．前記第一の一方向関数f_1（ｘ）と前記第二の一方向関数f_2（ｘ）が同一であることを特徴とする請求の範囲３に記載の電子通貨システムの実施手法。

５．第一のプレイメージx_1と目隠しされない形式の第二のイメージf_2（x_2）とを前記第二の当事者に送信する手段が匿名で行われることを特徴とする請求の範囲４に記載の電子通貨システムの実施手法。

６．前記第二の当事者が銀行であることを特徴とする請求の範囲５に記載の電子通貨システムの実施手法。

７．電子通貨システムの実施手法であってさらに、

第三の当事者からの購入品あるいはサービスに対する支払いとして第二のプレイメージｘ２が第三の当事者に送られる手順を含むことを特徴とする請求の範囲３

に記載の電子通貨システムの実施手法。

８．電子通貨システムの実施方法であってさらに、

第三の当事者の署名鍵と第一のプレイメージx_1を結合してひとつの情報のブロックを作成する手順、

前記情報のブロックを第二の当事者の暗号鍵を使って暗号化しで暗号化された情報のブロックを生成する手順、

前記暗号化された情報のブロックを第三の当事者に送る手順

とからなることを特徴とする請求の範囲１に記載の電子通貨システムの実施手法。

９．電子通貨システムの実施手法であって、

第一の当事者から

第一の一方向関数f_1（ｘ）を用いて第一のイメージf_1（x_1）を生成する元の値（であって、

かつ第二の当事者があらかじめ決められた金額を前記プレイメージx_1を第二の当事者に申告した当事者に信用貸しする確約と結合される第一のプレイメージを受け取る手順、

第二のプレイメージx_2を選択する手順、

第二の一方向関数f_2（ｘ）を使って第二のプレイメージx_2から第二のイメージf_2（x_2）を生成する手順、

第一のプレイメージx_1と目隠しされない形式の第二のイメージf_2（x_2）を第二の当事者に送る手順、

第二の当事者から

ディジタル署名を含む文書であって、

前記文書は第二の当事者が前記あらかじめ決められた金額を前記プレイメージｘ２を第二の当事者に申告した第一の当事者に信用貸しする確約を意味する文書を

受け取る手順とから成ることを特徴とする電子通貨システムの実施手法。

１０．前記第一の一方向関数f_1（ｘ）と前記第二の一方向関数f_2（ｘ）が同一であることを特徴とする請求の範囲９に記載の電子通貨システムの実施手法。

１１．第一のプレイメージx_1と目隠しされない形式の第二のイメージf_2（x_2）とを前記第二の当事者に送信する手段が匿名で行われることを特徴とする請求の範囲９に記載の電子通貨システムの実施手法。

１２．電子通貨システムの実施手法であって、

第一の当事者から

第二の当事者の公開署名鍵と第一のプレイメージx_1を結合し一つの情報のブロックとし、前記情報のブロックを第三の当事者の暗号鍵を用いて暗号化することによって生成された暗号化された情報のブロックを受け取る手順、

第二のプレイメージx_2を選択する手順、

第二の一方向関数f_2（ｘ）を使って第二のプレイメージx_2から第二のイメージf_2（x_2）を生成する手順、

前記暗号化された情報のブロックと前記イメージｆ（x_2）を一緒にして目隠しされない形式でメッセージを形成する手順、

前記メッセージを第三の当事者へ送る手順、

第三の当事者から

ディジタル署名を含む文書であって、

前記文書は第三の当事者があらかじめ決められた金額をプレイメージx_2を第三の当事者に申告した第一の当事者に信用貸しする確約を意味する文書を受け取る手順とから成ることを特徴とする電子通貨システムの実施手法。

１３．前記第一の一方向関数f_1（ｘ）と前記第二の一方向関数f_2（ｘ）が同一であることを特徴とする請求の範囲１２に記載の電子通貨システムの実施手法。

１４．前記メッセージが第三の当事者に送られる前に

第三の当事者が所有している公開署名鍵と対応する秘密の署名鍵を使って署名を行う手順により署名が行われる手順を含むことを特徴とする請求の範囲１２に記載の電子通貨システムの実施手法。

１５．第二の当事者が第一の当事者から暗号化された情報のブロックを受け取る

ことを特徴とする請求の範囲１２に記載の電子通貨システムの実施手法。

１６．電子通貨システムの実施手法であって、

第一のエンティティから

第一の一方向関数 f_1（x）を用いてプレイメージ x_1 から生成された目隠しされない形式のイメージ f_1（x_1）を受け取る手順、

あらかじめ決められた金額をプレイメージ x_1 の第一の申告者に信用貸しするという確約を含むメッセージを生成する手順、

前記メッセージにディジタル署名を行う手順、

第一の当事者に前記メッセージと前記ディジタル署名を送る手順とから成ることを特徴とする電子通貨システムの実施手法。

１７．受信する当事者が第一のエンティティの口座を維持し

前記プロトコルがあらかじめ決められた金額を第一の当事者の口座の借方に記入する手順を含むことを特徴とする請求の範囲１６に記載の電子通貨システムの実施手法。

１８．前記電子通貨システムの実施手法がさらに続いて、

第三の当事者からプレイメージ x_1 を受信する手順、

前記プレイメージ x_1 をデータベースで調べる手順、

プレイメージ x_1 を前記データベースで検出しなかった場合に第三の当事者に予め決められた金額の信用貸しを行う手順、

プレイメージ x_1 を前記データベースに加える手順とからなることを特徴とする請求の範囲１６に記載の電子通貨システムの実施手法。

１９．前記電子通貨システムの実施手法がさらに続いて、

プレイメージ x_1 と

一方向関数 f_2（x）を用いてプレイメージ x_2 から生成された目隠しされない形式のイメージ f_2（x_2）を

第三の当事者から受信する手順と、

前記プレイメージ x_1 をデータベースで調べる手順と、

プレイメージ x_1 を前記データベースで検出しなかった場合にディジタル署名を含む署名された文書であって前記プレイメージ x_2 の第一の申告者に前記あらかじめ

決められた金額を信用貸しする確約を示す文書を生成する手順、

プレイメージx_1を前記データベースに加える手順とからなることを特徴とする

請求の範囲１６に記載の電子通貨システムの実施手法。

２０．前記第一の一方向関数f_1（ｘ）と前記第二の一方向関数f_2（ｘ）が同一

であることを特徴とする請求の範囲１９に記載の電子通貨システムの実施手法。

２１．第二の当事者から

第三の当事者の暗号鍵と第一のプレイメージx_1とをひとつの情報のブロックに

結合して生成され、第一の暗号鍵を用いて前記情報のブロックを暗号化しで暗号

化された第一のブロックを形成し、一方向関数f_2（ｘ）を用いでプレイメージ

x_2から生成された目隠しされない形式のイメージf_2（x_2）と前記暗号化され

た第一の情報のブロックを結合したメッセージを受信する手順、

前記暗号化された第一の情報のブロックを解読する手順、

ディジタル署名を含む文書であって、前記プレイメージx_2の第一の申告者に予

め決められた金額の信用貸しを行うという確約を表した文書を作成する手順、

前記文書を第二の当事者に送る手順とからなることを特徴とする請求の範囲１６

に記載の電子通貨システムの実施手法。

２２．前記第一の一方向関数f_1（ｘ）と前記第二の一方向関数f_2（ｘ）が同一

であることを特徴とする請求の範囲２１に記載の電子通貨システムの実施手法。

２３．前記電子通貨システムの実施手法がさらに、

プレイメージx_1をデータベースで調べる手順、

プレイメージx_1を前記データベースで検出しなかった場合にのみ署名された文

書を作成する手順、

プレイメージx_1を前記データベースに加える手順とからなることを特徴とする

請求の範囲２１に記載の電子通貨システムの実施手法。

２４．電子通貨システムの実施手法であって、

第一のイメージｆ（x_1）と

予め決められた貨幣価値と関連づけられた第一のプレイメージx_1とを入手する

手順、

第二のプレイメージx_2を選択する手順、

第二の一方向関数 f_2（x）を用いて第二のプレイメージ x_2 から第二のイメージ f_2（x_2）を生成する手順、

第一のプレイメージ x_1 と目隠しされない形式の第二のイメージ f_2（x_2）を第二の当事者に送る手順、

第二の当事者から

ディジタル署名を含む文書であって

第二の当事者が予め決められた金額であって前記予め決められた貨幣価値を超えない金額を

第二の当事者に前記第二のプレイメージ x_2 を最初に申告した者に信用貸しするという確約を表した文書を受け取る手順からなることを特徴とする電子通貨システムの実施手法。

２５．前記予め決められた金額が前記予め決められた貨幣価値よりも少ないことを特徴とする請求の範囲２４に記載の電子通貨システムの実施手法。

２６．前記第一の一方向関数 f_1（x）と前記第二の一方向関数 f_2（x）が同一であることを特徴とする請求の範囲２４に記載の電子通貨システムの実施手法。

２７．電子通貨システムの実施手法であって、

第一のイメージ f（x_1）と

予め決められた貨幣価値と関連づけられた第一のプレイメージ x_1 とを入手する手順、

正の整数１からｎの値を持つ多数のプレイメージ x_1 を選択する手順、

第二の一方向関数 f_2（x）を用いて第二のプレイメージ x_1 から多数のイメージ f_2（x_1）を生成する手順、

第一のプレイメージ x_1 と目隠ししない形式ですべてのイメージ f_2（x_1）を第二の当事者に送る手順、

第二の当事者から

各文書がディジタル署名を含み前記文書の数はイメージ f_2（x_1）と同じである多数の文書であって予め決められた額が多数記載されており、

前記多数の文書のそれぞれには第二の当事者が

プレイメージ x_1 の第一の申告者に対して

異なった額の前記予め決められた額が多数記載されているもののうち前記プレイメージx_1と対応する額を信用貸しするという確約を表した文書を受け取る手順とから成り、

前記予め決められた額の総計が前記予め決められた貨幣価値と等しいことを特徴とする電子通貨システムの実施手法。

２８．電子通貨システムの実施手法であって、

第一のイメージｆ（x_1）と

予め決められた貨幣価値と関連づけられた第一のプレイメージx_1とを入手する手順、

第一のプレイメージx_1と第二の当事者の署名鍵を結合して一つの情報ブロックを作成する手順、

前記情報ブロックを第三の当事者の暗号鍵を用いて暗号化さ机た情報のブロックとして生成する手順、

第三の当事者に暗号化された情報のブロックを送る手順とから成ることを特徴とする電子通貨システムの実施方法。

２９．前記電子通貨システムの実施手法がさらに、

第二の当事者のその他の情報と署名鍵と第一のプレイメージx_1をひとつの情報のブロックに結合する手順を含むことを特徴とする請求の範囲２８に記載の電子通貨システムの実施手法。

３０．電子通貨システムの実施手法であって、

一方向関数f_2（x_2）を用いてプレイメージx_2から生成された

目隠しされない形式のイメージf_2（x_2）を

第二の当事者に送る手順と、

第二の当事者から

ディジタル署名を含む目隠しされない形式の文書であって

前記プレイメージx_1を最初に申告した者に対し予め決められた金額の信用貸しを行うという確約を表した文書を受け取る手順、

第二の当事者から前記目隠しされない形式のノートを受け取った応答として品物やサービスを第三の当事者に提供することを許可する手順とから成ることを

特徴とする電子通貨システムの実施手法。

【手続補正書】

【提出日】１９９９年3月１０日（１９９９．３．１０）

【補正内容】

請求の範囲

１．電子通貨システムの実施方法であって、

一方向関数ｆ１（ｘ）を用いて演算前の元の値であるプレイメージｘ１から演算後であるイメージｆ１（ｘ１）を生成する手順、

イメージｆ１（ｘ１）を見える形式で第二の当事者に送信する手順、

前記第二の当事者からディジタル署名を含む文書を受信する手順、

から成り、

第二の当事者に対するプレイメージｘ１の最初の申告者にあらかじめ決められた金額を前記第二の当事者が信用貸しするという確約を前記文書が表すことを特徴とする電子通貨システムの実施方法。

２．電子通貨システムの実施方法であって、

第一のイメージｆ（ｘ１）と

予め決められた貨幣価値と関連づけられた第一のプレイメージｘ１とを入手する手順、

第一のプレイメージｘ１と第二の当事者の署名鍵を結合して一つの情報ブロックを作成する手順、

前記情報ブロックを第三の当事者の暗号鍵を用いて暗号化された情報のブロックとして生成する手順、

第三の当事者の暗号鍵を用いて前記情報ブロックを暗号化し、暗号化された情報ブロックを生成する手順、

第三の当事者に暗号化された情報ブロックを送る手順とから成ることを特徴とする電子通貨システムの実施方法。

【手続補正書】

【提出日】１９９９年4月6日（１９９９．４．６）

【補正内容】

明細書

追跡不可能な電子通貨

背景技術

この発明は、電子通貨システム一般に関する。

電子通貨システムの直観的にわかる最終的な形態は、有形の現金の最良の特徴（プライバシーが守られる、匿名性、偽造しにくい）と、電子取り引きの持つ最良の特徴（速さ、簡便性、輸送や保管に対する潜在的な安全性）を合わせ持った形態である。匿名性を有す電子通貨システムを実現するための基本的な問題は、次のように単純化することができる。２つの連続した取り引きにおいで、この電子通貨の所有者が識別できなかったならば、この所有者が第一の取り引きがなかったように振る舞い、同じ電子コインを再び使用することをどうやって防ぐかという問題である。この問題に対する第一の解決方法は、チャーム、フィアットとノアーによって提案されている（D．チャーム(D.Chaum)、A．フィアット(A.Fiat)、M．ノアー(M.Noar)著、アントレーサブル・エレクトロニック・キャッシュ(Untracedable Electtronic Cash)、Pvoc. CRYPTO'88、Springer-Verlag(1990)、319-327ページ）。これは、同じ電子通貨が２回、中央の銀行に送られてきた場合には、通貨の二重使用を検出して二重使用を行った人の特定が十分に行えるということを前提条件として成立している。他の解決方法の提案のうちのいくつかにもこの前提が用いられていて、銀行は各取り引きを複雑にする必要がないという利点を有す。しかしながら実際には、この前提条件には重大な欠点がある。それは不正な取り引きは発生後しばらくたってから検出されるということであり、不正実行者が法によって処罰されないという確信があれば（アクセスできない状態であったり、第三者のＩＤや電子通貨を使っている場合など）、不正実行者は意のままに電子通貨の二重使用をすることができる。

しかしながら、このような電子通貨の不正使用を防止するには、二重使用の検出や、二重使用に対して警告を発することができるように、取り引きが発生する毎に何らかの確認をいずれかの方法で行う必要がある。それでは、どのようにし

て匿名性を保護するのか。ひとつのアプローチとして、中身にいたずらできないように作られたハードウエアを基礎として、電子通貨を使う人が正直に（すなわち、電子通貨の二重使用をしない）しなければならないよう強いる方法がある(例えば、Ｓ．イーブン(S.Even)、Ｏ．ゴールドリッチ(O.Goldreich)、Ｙ．ヤコブ(Y.Yacobi)著、エレクトロニックウォーレット(Electronic Wallet,Proc. CRYPTO'83、Plenum Press(1984)、383－386ページを参照のこと)。しかしながらこのような前提に基づいた方法は、非常にもろい。もし誰かがハードウエアの不正操作に成功したらならば、その不正使用者が通貨の二重使用ができるばかりでなく、ハードウエアに隠された情報を手に入れる（たとえば、購入したり、偶然によって）ことができれば、誰でもがどこからでも勝手に高額な金額を使うことができるようになる。従来の不正使用防止技術は、前述のようなリスクを有すものを基礎としたものであるため、信頼できる技術ではない。

その他のアプローチとして、暗号による方法がある。例えば、ある強力な暗号法のもとでは、「目隠しされた」通貨と、後で正規通貨であると認証できるが、どのように特殊なプロトコルを実行させても接続できない情報を造るプロトコルを構築することが可能となる。（例として、Ｄ．チャーム(D.Chaum)著、プライバシー・プロテクト・ペイメント(Privacy Protected Payments--Unconditinal Payer and/or Payee Untraceability,SMART CARD 2000: The Future of IC CardsOOProc.ifip wg 11.6 Int'l Conf.,North-Holland(1989)，ページ69-93)、及びＤ．チャーム(D.Caum)著、オンライン・キャシュ・チェック(Online Cash Checks)、Proc.EUROCRYPT'89、Springer-Verlag(1989)、288-293ページを参照のこと）

発明の開示

この発明は、簡単で実用的なオンライン電子通貨システムであって、匿名性を有し追跡不可能な情報伝達が可能なネットワークを基礎とした電子通貨システムを実現するものである。概して、この発明には２つの簡単な基本要素である、一方向関数と署名機構を用いている。どちらもよく知られた技術であって、詳細については、一般に入手できる暗号に関する本で知ることができる。例えば、ブル

ース・シュネイヤー（Bruce Schneier）著、アプライド・クリプトグラフィー（Applied Cryptography）（１９９４年　ジョン・ウィリー・アンド・サンズ 社（John Wiley & Sons, Inc.）刊にある。このシステムは、電子通貨を使う人の匿名性を保護することはもちろん電子通貨の正当性を保証するものであるばかりでなく、偽造することはできず、また１回しか使用できない。

本発明の一形態である電子通貨プロトコルは、一方向関数f_1（x）を用いて変換前の元の値であるプレイメージx_1から変換後の値であるイメージf_1（x_1）を生成する手順、イメージf_1（x_1）を目隠ししない形式で第二の当事者に送信する手順、第二の当事者からディジタル署名を含む文書を受け取る手順とから成る。前記受け取った署名を含む文書は、第二の当事者が、第一のプレイメージｘ１を決めた者に対してあらかじめ決められた金額を信用貸しするという確約を意味する。

本発明の最良の形態は、次に示すような形態を含む。本発明の電子通貨プロトコルはまた、第三の当事者から購入した商品や受けたサービスに対する支払いとして、プレイメージx_1を第三の当事者へ送る場合も含んでいる。またさらに、第二のプレイメージx_2を選択し、第二の一方向関数f_2（x）により第二のプレイメージx_2を第二のイメージf_2（x_2）に変換し、第一のプレイメージx_1と目隠ししない形式で第二のイメージf_2（x_2）を第二の当事者に送信し、第二の当事者からディジタル署名を含む文書を受信するという形態もある。前記文書は、第二の当事者が、第一のプレイメージx_2を決めた者に対してあらかじめ決められた金額を信用貸しするという確約を意味する。どちらの場合も、f_1（x）とf_2（x）は同じ関数である。後者の場合、第二の当事者に対して第一のプレイメージx_1と目隠ししない形式で第二のイメージf_2（x_2）を送信しているのは、匿名性を保持するためであり、第二の当事者は銀行である。

また、本発明の最良の形態であるプロトコルには、第三の当事者の署名鍵と第一のプレイメージx_1を結合して情報をひとつのブロックに構成する手順、前記情報ブロックを第二の当事者の暗号鍵を使って暗号化して、暗号化された情報ブロックとする手順、前記暗号化された情報ブロックを第三の当事者に送信する手順とから成るものがある。

その他の形態である本発明の電子通貨プロトコルは次の手順で行われる。まず第一の当事者から第一のプレイメージx_1を受け取る手順であり、このプレイメージx_1は第一の一方向関数$f_1(x)$によって処理され第一のイメージ$f_1(x_1)$となる。前記第一のプレイメージx_1は、第二の当事者が前記第一のプレイメージx_1を第二の当事者に申告した第一の当事者に対して、予定額の信用貸しを行うという、第二の当事者による確約と連結している。さらに、第二のプレイメージx_2を選択する手順、第二の一方向関数$f_2(x)$により第二のプレイメージx_2から第二のイメージ$f_2(x_2)$を生成する手順、第一のプレイメージx_1と目隠しされない形式の第二のイメージ$f_2(x_2)$を第二の当事者に送信する手順、第二の当事者からディジタル署名を含むノートを受信する手順とから成る。このノートは、第二のプレイメージx_2を第二の当事者に送った第一の当事者に対し、予定の額の信用貸しを行うという第二の当事者の約束を表わしている。

さらなる他の形態では、本発明の電子通貨プロトコルは次の手順で行われる。まず、第一の当事者から暗号化された情報のブロックを受け取る手順であり、この情報が暗号化されたブロックは、第二の当事者の公開署名鍵と第一のプレイメージx_1とを連結して情報のブロックが構成され、さらに前記情報のブロックは第三者の暗号鍵を使って暗号化されたものである。続いて、第二のプレイメージx_2を選択ずる手順、第二の一方向関数$f_2(x)$を用いてプレイメージx_2からイメージ$f_2(x_2)$を生成する手順、前記暗号化した情報ブロックとイメージ$f_2(x_2)$を含むメッセージを目隠ししない形式で作り上げる手順、前記メッセージを第三の当事者に送る手順、第三の当事者からディジタル署名を含むノートを受け取る手順から成る。このノートは、第二のプレイメージx_2を第三の当事者に送った第一の当事者に対し、予め決められた額の信用貸しを行うという第三の当事者の確約を表わしている。

さらなる他の形態では、本発明の電子通貨プロトコルは次の手順で行われる。第一のエンティティから一方向関数$f_1(x)$をプレイメージx_1に適用して生成され、かつ目隠しされない表記形式のイメージ$f_1(x_1)$を受信する手順、プレイメージx_1を送った第一の当事者に対し、予め決められた額の信用貸しを行うという確約を含むメッセージを作成する手順、前記メッセージにディジタル署名

で

署名する手順、前記メッセージをディジタル署名と一緒に前記第一の当事者に送信する手順、とである。

本発明の電子通貨プロトコルの最良の実施の形態ではさらに続いて、第三の当事者からプレイメージx_1を受け取る手順、プレイメージx_1をデータベースで調べる手順、もしプレイメージx_1がデータベースになかったら、あらかじめ決められた金額を第三の当事者に信用貸し、プレイメージx_1をデータベースに加える手順が含まれている。あるいは本発明の電子通貨プロトコルがさらに続いて、プレイメージx_1と目隠しされない形式のイメージf_2（x_2）であって一方向関数f_2（x）をプレイメージx_2に適用して生成されたイメージを第三者から受け取る手順、プレイメージx_1をデータベースで調べる手順、もしプレイメージx_1がデータベースになかったら、あらかじめ決められた金額をプレイメージx_2を送った第一の当事者に信用貸しするという確約を示し、ディジタル署名も添付されているノートを作成する手順、プレイメージx_1をデータベースに加える手順から成るプロトコルであってもよい。

また本発明の最良の実施の形態として、次に示すメッセージを第二の当事者から受け取ることを特徴とするものがある。前記メッセージは、第三の当事者の暗号鍵と第一のプレイメージx_1とを結合してひとつの情報のブロックとして形成し、前記情報のブロックを第一の暗号鍵を使って暗号化された第一のブロックを生成し、前記暗号化された第一のブロックをプレイメージx_2を一方向関数f_2（x）を用いて生成される目隠ししない形式のイメージf_2（x_2）と結合することによって得られる。さらに、暗号化された第一の情報のブロックを解読する手順、ディジタル署名を含み、第一のプレイメージx_2の申告者にあらかじめ決められた金額を信用貸しするという確約を表わしたノートを生成する手順、前記ノートを第二の当事者に送る手順を有している。

また、さらに他の形態として、次の手順を有する電子通貨プロトコルがある。一方向関数f_2（x）を用いてプレイメージx_2から生成され目隠しされない形式のイメージf_2（x_2）を第二の当事者に送る手順、第二の当事者から署名された

ノートであって、目隠しされない形式で、ディジタル署名を含み、最初にプレイメージx_2を申告した者に対して決められた金額の信用貸しを行う約束を表わした

ノートを受け取る手順、さらに前記目隠しされない形式のノートを第二の当事者から応答として受け取り、品物やサービスを第三の当事者へ配達するのを認める手順とがある。

本発明は、簡単で安価な、擬似貨幣による取り引きの方法を提供するものである。交換（例えば貨幣の引き出し）といった項目では、実際の貨幣と同じ特性を持つ。例として、本発明は、（１）大体において匿名性が保証されている、（２）安全で、（３）安価で使うことができ、（４）持ち運びが簡単で交換も容易である、という特徴がある。

関係者は、ある特定の貨幣に対するx_1の値を貨幣を使うまで秘密にしておくことにより、その貨幣支払いの取り消しといった不正な銀行の背信行為から守られている。特定の金額ｆ（x_1）が公にかつ匿名でなく預金されでいる限り、x_1と結合している支払いが行われるまで、銀行には道義心が要求される。もちろん、銀行は、受け取ったx_1がすでに使われた貨幣に関したものであると主張して、実際の交換処理中に匿名での交換処理を取り消しを行うことができる。しかしながら、銀行は誰がこのような「食い逃げ」計画によってだまそうとしたか知ることができない。それ故、銀行はモニターや一般に公表されることに対しで無防備である。

最終的に、電子通貨の署名に用いられるディジタル署名手法の有す安全性により、銀行も電子通貨の偽造から守られる。さらに加えて、銀行は、貨幣に対するx_1の値を永久に保存していることにより、「二重使用（あるいは二重支払い）」を防止する。

その他の利点や特徴は、以下の発明の実施するための最良の形態及び請求の範囲において明らかにする。

図面の簡単な説明

第１図は、匿名でない電子通貨の引き出しプロトコルを示す図である。第２図

は、電子通貨の匿名での交換プロトコルを示す図である。第３図は、電子通貨での匿名での商品購入プロトコルを示す図である。第４図は、匿名でない電子通貨の預金プロトコルを示す図である。第５図は、電子通貨の匿名での支払いプロトコルの他の形態を示す図である。第６図は、匿名あるいは匿名でないドロップ・ペイメントまたは為替プロトコルを示す図である。第７図は、暗号化した為替プロトコルを示す図である。

発明を実施するための最良の形態

匿名で通信する能力は、いろいろな意味で、匿名の金銭取り引きが行われる場合には優先されなければならない事項である。なぜなら、ある団体の通信についての情報は、その団体の商取り引きに関する情報を明らかにしてしまうからである。実際には、通信の匿名性が基礎としているのは、電話会社が自社のシステムの秘密性を保護しているという信頼にすぎない。各団体は正体のわからない匿名での返信者を信頼するか、あるいは文献から公に入手できる他の技術のひとつを装備して信頼するかの選択ができる。

団体間の通信は第三者に対して匿名性を持つばかりでなく、その団体間でも互いに匿名性を持って通信を行うことを想定する。（代表的な実施例において、後者の形態は自己認識を除いて前者の自然な結果である。）このような条件における、簡単で幾分匿名性を有す電子通貨システムのプロトコルを第１図に示す。

以下で説明するさまざまなプロトコル（第１図から第７図を参照のこと）では、３団体を顧客１０と売り主２０と銀行３０という名称で定義する。顧客１０は、もちろん一般的には支払人の代表であり、売り主２０は一般的には受取人の代表である。当然ではあるが、この設定は説明を明快にする目的で決めたもので、この発明の範囲を限定するものではない。従って当然ながら、この三者を集団Ａ、集団Ｂ、集団Ｃとして引用しても同じ効力を持つ。

図には、いくつかの異なった団体がブロックによって示されており、ある団体から他の団体への情報の伝達は該当するブロックをつなぐ線によって示している。各線は、ある団体から他の巣団へ一定の情報が伝わることを示しており、線の端の矢印が通信の方向を示している。伝達される情報は、内容をまとめたシンボ

ルとして、線の下に示してある。

各ブロックにはラベルが付けられ、次に示すような特定の物として記述されているが、前記特定の物による処理は、コンピュータ処理や通信を実行するコンピュータ機器によって実行されるものである。コンピュータ機器は、多岐にわたる種類の電子機器を含んでいる。例えば、パーソナル・コンピュータ、ＰＣカード（ＰＣＭＣＩＡ対応カード）、ＰＤＩ、スマートカード、パームトップコンピュータ、強力なワークステイション等でありこれらはその一部に過ぎない。次に説明するように、プロトコルの銀行側の処理は、現在ＡＴＭによるトランザクションを処理しているサーバと同様に、電子商取引を処理するようにプログラムされたサーバによって実行される。前記サーバは、データの到着する複数の電話線を有し、関連データを保存するためのデータ記憶容量を持っていることが望ましい。

コンピュータ機器が内部あるいは外部に、プロトコルを実行するするために必要なプログラムやデータのために必要なメモリを有していることは当然のことである。さらに、前記コンピュータ機器は、例えばモデムのような、他のコンピュータ機器と通信を行うための手段も有す。さらに付け加えれば、情報を伝送する通信媒体は非常に多くの可能性を持っている。媒体の例としては、電話線、ケーブル、インターネット、衛星通信、無線通信などが挙げられる。言い換えれば、本発明は、使われている機器の種類や採用している通信方法によって限定されるものではない。可能性や組み合わせは、人の創作力によって限定されるものである。

これから説明するプロトコルにおいては、銀行３０が公に使用できる一方向関数ｆ（ｘ）を、選択し、制定する。このような関数は、誰もが商取引においてアクセスし使うことができるように、誰でもが公に入手できるものでなくてはならない。一般に、一方向関数は、x_1を使ってｆ（x_1）を算出することはできるが、ｆ（x_1）を与えられてもx_1を算出できない関数ｆ（ｘ）を意味する。以下の説明では、x_1はｆ（x_1）のプレイメージと、ｆ（x_1）はx_1のイメージとする。

実際には、完全な一方向関数は存在しない。現在一方向関数と考えられているずべての関数は、コンピュータの能力や手法によってｆ（ｘ１）からｘ１を決定することが十分にできる。それゆえ、一方向関数という語には、ｆ（ｘ１）からｘ１を算出することが、不可能である必要はないが非常に難しい関数であるという意味も含まれる。

一方向関数は、標準のハッシュ関数（例えば、ＭＤ５、ＳＨＡ等）のうちのいずれかでよい。さらにつけ加えれば、いくつかの一方向関数を使うことも、これを結合することも可能である。この技術分野において、多くの種類の一方向関数が知られている。その中の幾つかは、コンピュータに移植することが簡単で、スマートカードに装備することもできる。

以上の基礎知識を前提として、本発明の実施の形態となる種々のプロトコルについて説明する。まず、顧客が銀行から「キャッシュ」を手に入れる処理に用いられる電子通貨の引き出しプロトコルから始める。

引き出しプロトコル

電子通貨の引き出し処理は、第１図に示した手法に従って行われる。顧客１０は、任意の数Ｘ１を選び、一方向関数ｆ（ｘ）を使って変換後の値であるｘ１のイメージを生成する。ｘ１の値は後処理装置が任意で行っているような乱数発生手段から得られた無作為の数列である。この数列は、例えば１２８ビット長のデータである。顧客１０は、支払い処理が発生してから完了するまでｘ１の値を秘密にしておく。

顧客１０は、金額とｆ（ｘ１）をまとめて銀行３０に送って引き出しの要求を行い、銀行３０から金を引き出す（匿名ではなく）。銀行３０は、明細書にディジタル署名を行って顧客の趣意に従う。このようにｆ（ｘ１）を正規の電子・通貨として認定し、要求の額を、顧客１０が銀行３０に持っている口座の借方に記入する。言い換えれば、銀行３０は、「最初にｆ（ｘ１）のプレイメージを決めた者に対して、総額ｚの信用貸しを行う」ことに関して銀行３０は署名を行って証明する、という効力を表わす明細書あるいは覚え書きを発行する。

署名や情報の認証を行う技術（例えば、秘密鍵と公開鍵のペアを使う方法）や

、ディジタル署名の手法は、よく知られている技術である。さらに詳しくは、この分野において広く認められた参考文献を参照すればよい。例えば、ブルース・シュネイヤー(Bruce Schneier)著、アプライド・クリプトグラフィー(Applied Cryptography)、１９９４年　ジョンウイリー・アンド・サンズ社(JohnWiley&Sons.Inc.)などである。

一般的に署名機構とは、文字にタグを付けるやり方のことである。典型的な例としては、公開鍵と秘密鍵のペアを使うものがある。公開鍵及び秘密鍵は、一方向関数を使って実行される。より現実的なアプローチ方法としては、さらに効果を上げるためにトラップ・ドア機能を使う方法がある（例えば、スキネイナー(Schneiner)著、ＲＳＡ、ＤＳＳ、エルガマ・アルゴリズム(RSA, DSS, Elgamal algorithms)参照のこと）。秘密鍵は、文字か文字列のいずれかを暗号化するのに使われ、文字に添付するディジタル署名として使われる。ディジタル署名は、自身の秘密鍵を持っている者の署名であることを示している。なぜなら、他者が前記文字列からこのような署名を作り出すことはできないからである。第二の当事者が公開鍵を使ってタグの暗号を解読すれば、署名者自身の秘密鍵によって署名がなされたことがわかる。この手法を保証するために、署名をした人の公開鍵を誰もが手に入れまた預けられてこと、かつ秘密鍵は危険にさらされることはないと信頼できることが、前提となっていることは明らかである。

公開鍵を公表すること、及び銀行３０が第一のｆ（x_1）のプレイメージを決めた者に対して明記された額を支払うという覚え書きにディジタル署名を添付したことにより、銀行３０はその責任を明らかにし、さらに偽造者から自身を守る。　銀行が発行した、証明書となる覚え書きをここではＣ（ｆ（x_1））と定義し、ノートと呼ぶ。このノートは顧客１０に返送される。さらに付け加えれば、ノートは公然と入手することができるが、x_1を知らない人にとっては何の価値もない。

交換プロトコル

関係者（例えば、顧客１０や売り主２０）は、いつでも、銀行３０において匿名で電子通貨の「交換」ができる。実際には、相手側当事者から電子通貨を受け

取ったら、処理を迅速に行うことが特に重要である。これは、電子通貨の正当な受取人の前に誰か他の者がx_1を銀行３０に送信してしまうリスクを最小にするためである。不正実行者は、複数の者に対してx_1を送信し、その電子通貨を複数回、送信しようとするかもしれない。そのようなことが起きたら、銀行３０に届いた最初の受取人がその価値を受け取り、その他の電子通貨の受取人達は該当しない電子通貨となり交換することができない。売り主２０にとっては、交換のタイミングはさほど重要でない。なぜなら、大体において売り主２０は、電子通貨の受

け取りが有効に完了するまでは、納入予定の品物やサービスを提供しないからである。　第２図に示したように、顧客１０が電子通貨を匿名で交換することを望んだと仮定すると、顧客１０は銀行３０にx_1と任意に選ばれたx_2の変換後のイメージである$f(x_2)$を送信する。言い換えれば、顧客１０はx_1によって前述したような引き出しプロトコルを行い、同時に引き出した総額を提供する。銀行３０は単に$f(x_2)$を認証し、$f(x_1)$は「すでに使われた」ということの証明としてx_1をデータベース４０に保存するだけである。これがx_1の二重使用されるのを防止する交換の手法である。

$f(x_1)$と$C(f(x_1))$はすでに銀行３０が所有しているので、銀行３０に対してx_1と$f(x_2)$といっしょにその情報を送ることは任意である。

プロトコルの銀行側処理がサーバーに実装されていれば、銀行は受信したx_1を自動的に保存する。さらに、銀行３０がもうひとつのx_1を受け取る毎に、最初にそれがすでに使われたもの（すなわち受信されたもの）であるかをチェックする。

誰が実際に電子通貨を使っているのかがはっきりわからない交換処理を、連続して取り扱うことができるようになる。交換処理には$f(x_2)$を明らかにすることのみが必要であり、x_2の持ち主を明らかにする必要はないことに注目してほしい。匿名を実現するための他の手法と違って、電子通貨を目隠しすること等その他の処理を必要としない。実際には、$f(x_1)$が目隠しされず、広く一般に知られていることが望ましい。

通信の匿名性を確保するよう求める手法は何でも、処理の匿名性が確保されれば十分に目的を果たす（すなわち、匿名性を実現することは可能であるが必須ではない）。

この手法は、電子通貨を両替する方法として使うこともできる。ｆ（x_2）を送信する代わりに、両替をしようとしている者は、複数のｆ（ｘ）の値（例えば、ｆ（x_2）、ｆ（x_3）、ｆ（x_4））を送信することができる。これらは、個々に特定の値を持ち、総合するとｆ（x_1）の値と関連する。銀行は、複数の署名付きノートであるＣ（ｆ（x_1））を返送する。

購入プロトコル

第３図に示したように、実際に電子通貨を支払うプロトコルは交換プロトコルと似ている。支払いを行う者（例えば顧客１０）は、受け取り人（例えば売り王２０）に、x_1を渡す。売り主２０は直接あるいはすぐにｆ（x_1）あるいはＣ（ｆ（x_1））にアクセスすることができないので、顧客１０は取引の一部の情報として送る。売り主２０は銀行３０に直接要求して、x_1を「フレッシュな」金銭に換える。この時当然に、銀行３０はx_1が以前に使われたものでないことを最初に確認する。売り主２０がこの交換処理を実施するときには、第２図に示した交換プロトコルを使う。前記交換処理が引き受けられた後、売り主２０は購入された品物あるいはサービスを顧客１０に提供する。

預金プロトコル

第４図に示したように、使用しない貨幣はいつでも、銀行３０に匿名でなく預金することができる。例えば、売り主２０が使わない貨幣ｆ（x_1）を預金しようとした場合、x_1を預金の要求と共に銀行３０に送信する。売り主２０は、ｆ（ｘ、）はもちろんＣ（ｆ（Ｘ１））を任意で送ってもよい。

x_1と預金要求を受け取ると、銀行３０はx_1が以前に銀行に送られてたことがあるかどうか、データベースを調べる。もちろん、以前に送られてきたことがあれば、銀行３０は売り主の請求書を信用せず、売り主２０に対して正規の電子通貨ではないことを報告する。銀行３０が以前にx_1を受信したことがなければ、あらかじめ決められ金額がある請求書を信用し、信用取引が登録されたことを確

認するために預金の受領書を売り主２０に送る。

プロトコルの拡張

以上説明した電子通貨手法における交換及び支払プロトコルには、いくつかの他の実施の形態の例がある。これら他の実施の形態は、求められている匿名性のレベルや関係に応じた有効な手段となるように作られている。例えば、第５図に示したのは、顧客１０が売り主２０よりも銀行３０にアクセスするほうが容易である場合、売り主２０は最初に顧客１０にｆ（x_2）を送り、顧客１０は売り主２０の代わりに交換プロトコルを行い、支払いの証明として署名された電子通貨

、

例えばＣ（ｆ（x_2））を返送する。前述したように、交換プロトコルは匿名で行われる。

あるいは、顧客１０及び売り主２０の双方が、お互いよりも銀行とよい関係をもっている場合、図６に示したような「ドロップ」ペイメントプロトコルを使うとよい。このプロトコルに従えば、顧客１０は売り主２０のための支払いを銀行に降ろし、売り主２０はその後すぐに銀行から支払いを回収する。

「ドロップ」支払いプロトコルの手順を以下に示す。最初に、顧客１０がある特定の額の貨幣の代わりとしてのx_1を銀行３０に送る。この時、売り主２０の公開署名鍵ｐ（ＰＳＫＰ）と取り引きに関する情報を付加して送る。いろいろな情報があるが、例えば、顧客１０が購入した品物を明らかにしたり取り引きを確認することを望んだ場合、さらに/あるいは売り主が支払いに関する顧客の意向を認めたといことを指示する場合などがあり、その結果、電子通貨が本質的な意味において、「電子為替」に変る。顧客１０は任意でｆ（x_1）とノートＣ（ｆ（x_1））を送ってもよいが、前述したように、この情報はすでに銀行３０が入手しているので、送る必要はない。

顧客１０が提供したその他の情報から集められた記録は、遠隔支払設定として特定の用途に使えるかもしれない。取り引きの性格が特に暗黙であるという場合でなければ、典型的には個人的な支払い方法になる。

もし、売り主２０が匿名性を保持することを望まなければ、公開署名鍵は売り主

２０のＩＤと明らかに関係しているものであってよいが、もし匿名性を望むのであれば、公開署名鍵はＩＤとはまったく関係ない特別な目的を有した公開鍵としなければならない。後者の場合には、公開鍵は信頼できる知人に極秘に渡すか、単純に匿名で公表する。

銀行３０はx_1に付随した第一の電子通貨ｆ（x_1）として表わされた総額を渡すことに同意し、以前に配布された公開署名鍵ｐと対応する秘密の署名鍵を使って署名されている。このようにして、顧客１０が購入しようとした品物の支払いを手に入れるために、売り主２０は、第１図に関連して以前に記述したプロトコルを使って、銀行３０から金を引き出す。このとき、売り主２０は任意のx_2を選択し、ｆ（ｘ）を使ってイメージｆ（x_2）を生成する。しかしながらこの例では、

売り主２０はｆ（x_2）を銀行３０に送信する前に秘密署名鍵を使ってｆ（x_2）に署名を行う。付け加えると、この場合、貨幣は売り主の口座から引き出されるのでなく、顧客１０によってこの処理の前に与えられた口座から転送するだけである。

銀行３０は売り主の公開署名鍵を使って、受信したｆ（x_2）が売り主２０（すなわち貨幣の転送を行った者）によって署名されことを確かめる。ｆ（x_2）の署名を確認すると、銀行３０は売り主２０に送信するノートＣｆ（x_2））を発行する。

金を受け取ったという確認のノートＣ（ｆ（x_2））を売り主２０が受け取った後、売り主２０は顧客１０に品物を送る。

もちろん理論上は、銀行３０は支払先に金を与える代わりに金を自分のものにすることによってだますことができる。しかしながら、支払人の匿名性を信頼している、あるいは少なくとも一般の人々が銀行３０が不正しないことをモニターしているので、支払人が取り引きを暴露する可能性をあてにすることができる。

関係者間の通信が傍受されているという設定のもとで、交換プロトコルを安全なものにする、とりわけ秘密のｘの値をが立ち聞きする者を通り抜けて通過するいくつかの方法がある。最も自然な方法は、公開鍵による暗号法である。関係者

が銀行のものはもちろんのこと互いの公開暗号鍵を知っていれば、銀行３０が送信するものを除くすべてのメッセージが、受信側の公開暗号鍵を使って暗号化するか、受信側の公開暗号鍵を使って暗号化された相称的な「セッションキー」を使っているかぎり、前述した全てのプロトコルが立ち聞きするものを絶滅させるように機能する。もちろん銀行のメッセージは、秘密でなくてよいよう考慮されている。なぜならメッセージは、x_1が誰か他の者によって秘密にされているｆ（x_1）という形式の署名された貨幣だけで構成されているからである。暗号化処理時にメッセージの認証コードやＭＡＣを使えば、メッセージが目的地に到着するまで送り主以外の誰かによっていたずらされることはないことが保証される。

公開暗号鍵の使用により、別の種類の「電子為替」が可能となる。この事例を第７図に示し、暗号化された電子為替プロトコルとして一般にあてはめる。顧客１０は、ある正規の電子通貨としての秘密のx_1の値を、売り主２０の公開鍵ｐと

その他の必要なＩＤや取引情報といっしょに暗号化する。前述の「ドロップ」プロトコルの場合と同様である。顧客１０はこの情報を、銀行の公開暗号鍵を使うか、あるいは銀行の公開暗号鍵を使って暗号化されたセッションキーを使って暗号化する。その後、顧客１０は暗号化された情報を直接売り主２０に送信する。

これを「現金」にするために、売り主２０は任意の値x_2を選び、そのイメージｆ（x_2）を生成し、顧客１０から受信したメッセージＥにｆ（x_2）を添付する。前と同様、ｆ（x_2）は銀行によって署名されると、それは売り主２０への金の移転を意味する。売り主２０は完了メッセージ（あるいは少なくともｆ（x_2））に、公開署名ｐに対応する秘密の署名鍵を使って署名を行い、Ｅとｆ（x_2）と署名を銀行３０に送る。任意で売り主２０はさらに、前述したような方法、すなわち銀行の暗号鍵あるいは付随的な相対鍵を使って、このメッセージを暗号化してもよい。

銀行３０は、自身の秘密鍵を使って売り主２０からのメッセージを解読した後、x_1がすでに保存されていないかデータベースを調べ、もし見つからなかった

場合には、銀行３０はx_1を保存する。さらに銀行３０は、ｆ（x_1）に関連した値に等しい額を売り主２０に振替えるという内容が記載されたノートＣ（ｆ（x_2））を生成する。前記ノートは売り主２０に送られ、領収書発行と確認が済んだ後、購入された品物は顧客１０に送られる。

実質的に、暗号化された最後のプロトコルは前述のものとほぼ同じである。暗号化が加えられたのは、支払人が受取人経由で「為替」を渡す処理においてであり、その間支払人の与えた秘密や付加情報は、中身がいたずらされていないことは保証される。

ノートＣ（ｆ（x_1））に処理が完了した日付を入れておくことは有益なことである。この場合、銀行30のデータベースに保存されているx_1はさほど大きくならない。これは、x_1を銀行のデータベースに永遠に保存しておく必要がないことによる。電子通貨の価値が失効しないように、スマートカード（あるいは顧客が取り引きをするために操作する装備すべて）は、自動的に古くなった電子通貨を新たな有効期限を持った新しい電子通貨に更新する。

満了日まで、電子通貨の払い戻しはできる。スマートカードの期限が過ぎて、

全てのｘ１を失っていしまった場合、期限満了後３ヶ月以内に申し立てておらず、ユーザすなわち顧客１０が電子通貨の価値に相当する額の信用貸しの要求を、銀行３０にｆ（x_1）と共にすることができる。しかしながら、一連のこの処理では、銀行との間で最初の通信であり、この場合には貨幣の引き出しを行っているときに、顧客１０は、自分自身であることを証明する。

プロトコルの顧客側は、x_1だけを保存すればよいので、スマートカードを使って簡単に装備することができる。また、一般的には、顧客は多くの金を必要としない。スマートカードを盗んだ者にx_1の値を盗まれないようにずるため、ＰＩＮが極秘にスマートカードに使われていて、x_1をアクセスする前にユーザが入力しなければならない。

以上記載した相互作用はすべて自動的に行われているのは当然のことであることに、注目してほしい。これらの処理は、適切なプログラムがされたコンピュータやプロセッサによって自動的に実行される。　コンピュータやプロセッサは、

取り引きを行う関係者によって実装され、その管理下にある。

その他の実施例は、以下に記載する。例として、秘密の値x_1を使って電子通貨と認証情報を結合するためのその他の手法がある。これもまでの記載では、秘密の値ｘ１は電子通貨を発行する人によって任意に生成されると仮定していた。しかしながら秘密の値は、一方向関数ｈ（ｘ）を用いて何らかの認証データのイメージを生成してもよい。この一方向関数は、あるいは通常の電子通貨の組み立てに使われる関数ｆ（ｘ）と同じであってもよい。認証情報は、用途、支払日、支払人の名前、予定の受取人といったもの、まとめていえば、支払人が銀行に保管しておきたいと思っているすべての情報、を含む。これらの情報は、ｈ（ｘ）を通して、秘密の値となるx_1を生成する。

この場合銀行は、前述の「ドロップ」あるいは「電子為替」プロトコルで行われた電子支払いで受信した取り引き情報を保存する必要はなくなる。本質的には、求められていることの全ては、払い込みが要求に応じて受取人を匿名にしないでラベル付けが行われることである。銀行が積極的に受取人の識別を行い、受取人のＩＤを含む取り引きの標準記録を保管していれば、支払人は後できちんと支払ったことを、ｆ（ｘ）に用いたx_1のプレイメージを公に明らかにすることによっ

て立証することができる。なぜなら、前記情報を示すｆ（ｘ）は、用途や支払日、支払人の名前、予定の受取人といった情報を含んでいるからである。x_1の値として普通に結合し、さらに他の電子通貨と交換して運ばれた暗黙の情報を、支払人は電子通貨と一緒に手に入れることができる。しかしながらこのような状況では、払い込み情報は暗黙のうちにx_1に含まれているため、銀行に送る必要ない。それゆえ、支払人が安全のため銀行を通過させなければならない情報は、受取人の認証に使われる公開署名鍵だけである。この情報は、暗黙のうちに支払人の要求で名前を明かして通信が行われる。

署名を基本とした通信を要求しているが、実際には、情報がx_1（あるいはｆ（x_1））とぴったりと一致していなければ、銀行は名前を明かして電子通貨を引き受けることはできないという趣旨により、受取人の身元の確認は排除される

。例として、いくつかのｘｉの特性（例えば、第１ビットが１であった場合）、銀行によって問題の電子通貨は名前を明らかにした場合のみ取り扱うという表明として公に宣言される。支払人は、ｆ（ｓｊ）によって秘密のｘｉを算出することができる。ｓｊは、特定の取引の情報と任意の値ｒを結合したものであり、その結果、ｘｉは非匿名性を持つことになる。このような性質のうち、およそ半分は、プレイメージｓｊをｆ（ｓ）で演算し、その結果として得られたある特定のデータ長を持つｆ（ｓｊ）によって決まるので、所望の効果を持つｘｉを見つけるまで、何回化のｒを選ばなければならない。このような電子通貨は、これを回収しようとする者は自身のＩＤを提供し、かつ銀行が納得するようにその証明をしなければならない、という性質を持つ。このため、銀行は通常の取引情報の一部として交換を申し出た者のＩＤを記録しておくことができる。この結果、この電子通貨を作成した者は、後にその起源と同様、その他の取り引きの詳細（起用予定も含めて）をも、銀行の取り引き記録を参照し、ｘｉを生成するのに用いられるｓｊを明らかにすることによって立証することができる。それゆえ、電子通貨を、余分の暗号や銀行に対しの情報を付加せずにまったく普通に使ったとしても、支払人には前述した「電子為替」によって必要な防護機能すべてが提供される。

請求の範囲

１．電子通貨システムの実施方法であって、

一方向関数ｆ１（ｘ）を用いて演算前の元の値であるプレイメージｘ１から演算後であるイメージｆ１（ｘ１）を生成する手順、

イメージｆ１（ｘ１）を見える形式で第二の当事者に送信する手順、

前記第二の当事者からディジタル署名を含む文書を受信する手順、

から成り、

第二の当事者に対するプレイメージｘ１の最初の申告者にあらかじめ決められた金額を前記第二の当事者が信用貸しするという確約を前記文書が表すことを特徴とする電子通貨システムの実施方法。

２．電子通貨システムの実施方法であって、

第一のイメージｆ（ｘ１）と

予め決められた貨幣価値と関連づけられた第一のプレイメージx_1とを入手する手順、

第一のプレイメージx_1と第二の当事者の署名鍵を結合して一つの情報ブロックを作成する手順、

前記情報ブロックを第三の当事者の暗号鍵を用いて暗号化された情報のブロックとして生成する手順、

第三の当事者の暗号鍵を用いて前記情報ブロックを暗号化し、暗号化された情報ブロックを生成する手順、

第三の当事者に暗号化された情報ブロックを送る手順とから成ることを特徴とする電子通貨システムの実施方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/14078

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL : 380/24
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/24, 23, 25, 29, 30, 49, 59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,914,698 (CHAUM) 03 April 1990.	1-30
A	US, A, 4,947,430 (CHAUM) 07 August 1990.	1-30
A	US, A, 4,949,380 (CHAUM) 14 August 1990.	1-30
A	US, A, 4,987,593 (CHAUM) 22 January 1991.	1-30
A	US, A, 4,991,210 (CHAUM) 05 February 1991.	1-30
A	US, A, 4,996,711 (CHAUM) 26 February 1991.	1-30
A	US, A, 5,131,039 (CHAUM) 14 July 1992.	1-30
A	US, A, 5,276,736 (CHAUM) 04 January 1994.	1-30
A	US, A, 5,373,558 (CHAUM) 13 December 1994.	1-30

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 OCTOBER 1996	25 FEB 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BERNARR EARL GREGORY Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*